NATIONAL
SECURITY
COMMISSION
ON ARTIFICIAL
INTELLIGENCE

# First Quarter Recommendations

MARCH 2020

# *Commissioners*

DR. ERIC SCHMIDT
*Chairman*

HON ROBERT O. WORK
*Vice Chairman*

SAFRA CATZ

DR. STEVE CHIEN

HON MIGNON CLYBURN

CHRISTOPHER DARBY

DR. KENNETH FORD

DR. JOSÉ-MARIE GRIFFITHS

DR. ERIC HORVITZ

ANDREW JASSY

GILMAN LOUIE

DR. WILLIAM MARK

DR. JASON MATHENY

HON KATHARINA MCFARLAND

DR. ANDREW MOORE

# *Contents*

# *Letter from Commissioners*

## March 2020

Trends in Artificial Intelligence (AI), including revelations about the power of AI for surveillance and its implications for weapons systems like swarming drones, indicate the United States is rapidly entering a new security environment. Since its inception, the National Security Commission on Artificial Intelligence (NSCAI) has been determined to match the pace of change and accelerate U.S. efforts to win the AI competition.

In November 2019, the NSCAI released its interim report assessing the state of the AI-national security landscape. We affirmed that the United States is in a strategic competition with AI at the center and that the future of our national security and economy are at stake. The report called for new imagination, common purpose, decisive action, and commitment from leaders in government, the private sector, and from society as a whole. It outlined the Commission's seven guiding principles:

- First, global leadership in AI technology is a national security priority.
- Second, adopting AI for defense and security purposes is an urgent national imperative.
- Third, private sector leaders and government officials must build a shared sense of responsibility for the welfare and security of the American people.
- Fourth, people are still essential. Talent remains the most important driver of progress in all facets of AI.
- Fifth, the power of free inquiry must be preserved.
- Sixth, ethics and strategic necessity are compatible with one another.
- Seventh, the American way of AI must reflect American values—including having the. rule of law at its core.

The report also issued 27 preliminary judgments and set the framework for the remainder of our research. Below, in this submission, the NSCAI provides an initial set of concrete recommendations that can be acted upon in the near term to spur progress.

No new information since the publication of the interim report changes our basic analysis of the challenges and opportunities presented by AI for national security. In the intervening months we have seen positive momentum and nascent action within the government to address core issues. We expressed optimism that public officials would support the necessary investments to sustain the United States' AI advantages. National security leaders continue to identify AI as a priority technology for improving business practices and defending the nation. The Justice Department is aggressively pursuing foreign threats to U.S. intellectual property[1]. The President's Budget calls for doubling non-defense AI research by 2022.[2] Congress continues to draft and debate new proposals for additional investment in AI-related research and infrastructure.

We expressed optimism that our leading companies and research universities would see the urgency of reconceiving their responsibilities and consider how their work impacts the health of

[1] See the DOJ Intellectual Property Task Force for further information, at https://www.justice.gov/iptf.

[2] See The White House, *President Trump's FY 2021 Budget Commits to Double Investments in Key Industries of the Future* (Feb 11, 2020), https://www.whitehouse.gov/briefings-statements/president-trumps-fy-2021-budget-commits-double-investments-key-industries-future/.

our democracy and future of our security. The government is working collaboratively with universities to help them maintain the integrity of their research against foreign threats.[3] We saw vitality in the American people's demand that their government pursue policies to maximize AI's potential, ensure the ethical and responsible use of AI, protect their civil liberties, and defend them from malicious use of the technology. In February, the Department of Defense took an important step by approving a set of ethical principles for AI.[4]

At the same time, we note concerning developments that amplify the importance of getting AI right for Americans. For example, a major news feature in January described an AI-empowered facial recognition program trained on publicly available data that appears to put the privacy of Americans at greater risk than is generally understood.[5] Other news reporting has demonstrated how effectively large sets of location data from cell phones can be combined with other available data to track the movements of individuals. In early March, a joint statement from multiple U.S. government leaders warned that "foreign actors continue to try to influence public sentiment and shape voter perceptions" in the United States, including by "spread[ing] false information."[6] As the Commission has argued, this could be exacerbated by AI-enabled digital manipulation. These developments only confirm that we need to develop best practices, policies, and laws aimed at ensuring the responsible development and fielding of AI-enabled systems and tools consistent with democratic norms and values.

## MOVING FORWARD: A DYNAMIC APPROACH TO COMMISSION IMPACT

A dynamic technology and dynamic national security environment require a dynamic approach to the Commission's work. Holding thoughts and ideas in abeyance for the next year until the Commission's final report will not serve the national interest or enhance our security. The NSCAI is on track to submit its final report in March 2021. However, the pace of AI development, the geopolitical situation, and the relevant authorization and budget timelines in 2020 represent important opportunities for the Commission to contribute to ongoing efforts to foster research and development, accelerate AI applications, and responsibly grapple with the implications of AI for our security, economy, and society. We have concluded that as we become confident in specific judgments and recommendations, the Commission should introduce them to the public and stakeholders on a quarterly basis.

We are releasing these recommendations shortly after the President's annual budget request, as Congress is considering authorizations and appropriations for FY 2021, and as departments and agencies are executing FY 2020 funding. In general, our funding proposals in areas that fall under the national defense budget category (050) require reprioritizing within the topline amounts for FY 2021, or reprogramming funds in FY 2020. By contrast, the non-defense discretionary spending we are proposing requires increases to agency toplines in the FY 2021 appropriations

[3] For example, through the Joint Committee on the Research Environment, organized by the White House Office of Science and Technology Policy.

[4] DoD, *DoD Adopts Ethical Principles for Artificial Intelligence*, (Feb. 24, 2020), https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/.

[5] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, New York Times (Jan. 18, 2020), sddhttps://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[6] See DOJ, *Joint Statement from DOJ, DOS, DOD, DHS, ODNI, FBI, NSA, and CISA on Preparations for Super Tuesday* (March 2, 2020), https://www.justice.gov/opa/pr/joint-statement-doj-dos-dod-dhs-odni-fbi-nsa-and-cisa-preparations-super-tuesday.

cycle to better support AI priorities. We detail our initial budgetary recommendations in the Tabs that follow.

The extraordinary ongoing global impact of the COVID-19 pandemic only confirms that the commission must retain flexibility and move quickly. Efforts to track and understand the virus—and to develop a vaccine—suggest the promise AI holds for keeping the nation safe at the intersection of technology, health, and national security.

## UNDERSTANDING THE SCOPE OF THIS MEMO

The NSCAI's first quarterly report of 2020 is a compendium of recommendations from across the Commission's lines of effort, which correspond to the Tabs attached to this memo and summarized below. It is not a comprehensive follow-up to the interim report and does not cover all areas that will be included in the final report. Rather it focuses on some areas the Commissioners identified as being most in need of attention, ripe for action, or foundational—and, therefore, important to outline now. It spells out recommendations that can inform ongoing deliberations tied to policy, budget, and legislative calendars. Each Tab can stand alone as a discrete memo on a specific dimension of the AI-national security nexus.

The Commissioners believe these recommendations are solidly grounded in analysis and ready for discussion with stakeholders. While the NSCAI anticipates no major deviations from the proposals or the underlying assessments, the Commission will adjust as any new information comes to our attention, and we will render our final judgments in March 2021.

As the Tabs illustrate, the breadth of the AI challenge is matched by the breadth of the NSCAI mandate, and is reflected in the breadth of recommendations introduced below. The Commission's recommendations here span research and development, workforce and training, national security application, hardware, 5G networks, alliance management, and ethical and responsible development and use.

## SUMMARY OF QUARTER 1 RECOMMENDATIONS:

This quarterly submission features recommendations divided into seven Tabs.

### 1. *Recommendations to Increase AI R&D Investments*

In Q1, the NSCAI focused on the FY21 R&D budget and identified funding recommendations that could have the greatest immediate impact on the United States' ability to maintain global leadership in AI R&D. Federal funding for AI has not kept pace with the growth or the potential of the field. The Commission assesses that the government should **immediately double non-defense AI R&D funding to $2 billion for FY 2021** in order to strengthen AI at our academic centers and national laboratories, and advance development across the broad network of government-sponsored and affiliated laboratories around **six key areas in the field where government support is critical to lay the foundation for our nation's future security.** This will support efforts to apply AI in government, develop technical and ethical standards for AI technologies, expand AI across fields of science and medicine, and build vital public-private partnerships. The government should also **launch a task force study and pilot program to establish a National AI Research Resource** in order to democratize AI by ensuring wider access to resource-intensive computation and large, curated data sets.

2. *Accelerate AI Application in DoD:*

   Q1 recommendations for applying AI focus on key organizational changes that can bolster existing initiatives and accelerate DoD AI application in the near term. The recommendations prioritize creating top-down leadership mechanisms to overcome structural barriers and enable strategic change. The Commission recommends that **DoD and the Office of the Director of National Intelligence (ODNI) establish a Steering Committee on Emerging Technology tri-chaired by the Deputy Secretary of Defense, the Vice Chairman of the Joint Chiefs of Staff, and the Principal Deputy Director of ODNI** in order to drive action on emerging technologies that otherwise may not be prioritized. The Steering Committee would assess novel threats related to emerging technology; connect strategic vision to organizational change; focus concept and capability development on emerging threats; guide defense investments that ensure America's strategic advantage against near-peer competitors; and provide authority to drive technology adoption and application. The NSCAI also recommends that **the Director of the Joint Artificial Intelligence Center (JAIC) should report directly to the Secretary of Defense** to ensure senior leadership oversight of DoD AI efforts and alignment with Department priorities, and that **the JAIC should continue to be led by a three-star general or flag officer with significant operational experience.**

3. *Strengthen AI Workforce:*

   Q1 recommendations target recruiting experts and developers, training end users, identifying internal talent, and educating those in support roles. They are premised on the belief that if the government cannot improve hiring practices, baseline knowledge, recruitment, and talent exchanges, we will struggle to accomplish any significant AI progress. The NSCAI proposes **expanding the Cyber Excepted Service; establishing AI Literacy course for Human Resource (HR) professionals; rebalancing the relationship between HR professionals, hiring managers, and organizational leaders; creating exemptions from OPM qualification policies; accelerating security clearance reviews for AI practitioners; expanding unclassified workspaces; piloting portfolio-based rather than resume-based hiring; mandating AI training; incentivizing self-development AI courses; incentivizing programming proficiency; including computational thinking in the Armed Services Vocational Aptitude Battery, or ASVAB; hiring professors part-time in government research labs; utilizing the pathways internship program; expanding the Cyber Corps/Scholarship for Service program; and increasing fellowships and partnership with industry.** If adopted, the recommendations would cumulatively change technologist hiring and talent management across the national security enterprise.

4. *Promote U.S. Leadership in AI Hardware & 5G:*

   Q1 recommendations lay the groundwork for long-term access to resilient, trusted, and assured microelectronics for AI advantage, and takes a portfolio-based approach to ensure that the United States continues running faster than potential adversaries in the field of cutting-edge microelectronics. The Commission recommends **expanding USG AI-enabling microelectronics programs** to develop novel and resilient sources for producing, integrating, assembling, and testing AI-enabling microelectronics; **stating research priorities, increasing USG R&D funding, and articulating a national strategy for microelectronics and associated infrastructure** in order to maintain global leadership in

AI-enabling hardware. The Q1 memo also provides limited, near-term recommendations to bolster U.S. fifth-generation cellular wireless (5G) capabilities, including by recommending **policies and funding opportunities that would advance spectrum-sharing and 5G commercial licensing, support R&D in critical technical areas, and further the development of open-access radio networks**, in order to accelerate 5G adoption in the United States and foster global alternatives to Huawei.

### 5. *Improve AI Cooperation Among Key Allies and Partners:*

Q1 recommendations focus on the role of the Five Eyes partnership as a vehicle for beginning to expand and institutionalize allied cooperative planning, data sharing, procurement, and interoperability for AI-enabled warfighting and intelligence efforts. The NSCAI recommends the government **establish a National Security Point of Contact for AI at a senior level, and encourage allied governments to do the same;** That person should **develop an allied assessment of comparative strengths in AI research and applications,** starting first with the Five Eyes, and then expanding to include NATO and other allies. Based on the assessment, the Point of Contact should **convene a multilateral working group for AI Collaboration and Interoperability, beginning with the Five Eyes, to develop a plan for deeper AI collaboration.** The Secretary of Defense should also designate a point of contact to **advance U.S. military concept and capability development cooperation with allies and partners to include AI wargaming, experimentation and pilot projects.**

### 6. *Advance Ethical and Responsible AI:*

Q1 recommendations concentrate on foundational, actionable steps and best practices the government should adopt in order to implement commonly agreed upon AI principles. The Commission recommends **integrating ethical and responsible AI training within general AI courses; sharing ethical and responsible AI training courses broadly with U.S. law enforcement organizations; establishing an expert body to brief the Federal government on emerging issues in AI ethics and responsibilities; developing strategies for documentation and engineering practices** in order to ensure traceability, auditability, accountability in the data, model, and system; and undertaking **self-assessments on resources for documentation and adequate multi-disciplinary support for AI procurement.**

### 7. *Threat Analysis and Recommended Actions:*

The purpose of the Commission's threat-oriented line of effort is to focus on AI and associated technology threats to the United States from foreign state and non-state actors. Due to the classified nature of the threat information, recommendations based on our analysis are classified and will be transmitted to Congress and the Executive Branch as an annex to this memo package.

# 1. Recommendations to Increase AI R&D Investments

TAB 1

Research is the lynchpin of America's global leadership in AI. However, as the Commission assessed in our Interim Report, the U.S. government's support for AI R&D has not kept pace with the field's revolutionary potential. As competitors accelerate their own investments and as the field grows in size and importance, the United States needs an injection of new resources to stay at the leading edge.

We have determined that this year, Congress should focus on bolstering non-defense AI R&D funding. Increasing funding for the National Science Foundation (NSF), Department of Energy (DOE), and other agencies, as we discuss below, would go a long way toward laying the groundwork for our future national security and economic competitiveness. We have also identified the priority research areas where this additive funding should be applied – areas of opportunity where we cannot rely on current levels of investment, given their importance to U.S. national security.

To advance nation-wide AI R&D infrastructure—and cultivate stronger connections between government, the commercial sector, and academia—we also propose piloting a National AI Research Resource that would serve to democratize access to AI R&D.

We encourage DoD and other agencies to leverage existing AI expertise to advance crucial AI development efforts through affiliated and sponsored research organizations, Federally Funded Research and Development Centers (FFRDCs),[7] and University Affiliated Research Centers (UARCs)[8]; and to cultivate AI expertise across the federal research enterprise.

DoD has identified AI as an advanced capability enabler and one of 11 defense modernization priorities.[9] In the FY2021 budget, DoD requested $800 million in AI developmental funding focused primarily on applications, and another $1.7 billion in AI-enabled autonomy.[10] These

[7] FFRDCs are government-owned, contractor-operated research centers designed to meet a "special long-term research or development need which cannot be met as effectively by existing in-house or contractor resources." DoD has 3 R&D FFRDCs: Lincoln Laboratory, Software Engineering Institute, and Center for Communications and Computing. Across the government, 12 agencies support a total of 42 FFRDCs. See NSF, *Master Government List of Federally Funded R&D Centers* (Mar. 2020), https://www.nsf.gov/statistics/ffrdclist/#agency.

[8] UARCs are strategic DoD research laboratories associated with universities that include education as part of their overall mission. These not-for-profit organizations maintain essential research, development and specific engineering core capabilities, and enter into long-term strategic relationships with their DoD sponsoring organizations. DoD sponsors 14 UARCs. See Defense Innovation Marketplace, *Federally Funded Research and Development Centers and University Affiliated Research Center*, https://defenseinnovationmarketplace.dtic.mil/ffrdcs-uarcs/.

[9] See DoD, Under Secretary of Defense for Research & Engineering, *Modernization Priorities*, https://www.cto.mil/modernization-priorities/.

[10] DoD has requested Joint AI Center (JAIC) funding be increased to $290 million, up from $242 million in FY 2020. At DARPA, where most basic DoD AI research is conducted, the FY 2021 AI budget request is for $459 million, an increase of $50 million from FY 2020. Moreover, DARPA has earmarked $2 billion for a multi-year research push on contextual AI – the next anticipated wave in AI research. See Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, *Defense Budget Overview* (Feb. 2020), https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2021/fy2021_Budget_Request_Overview_Book.pdf.

figures do not include significant AI R&D that occurs through the Military Services, via laboratories, affiliated organizations, and sponsored research.

These increases in AI research are welcome and urgently needed. However, the Commission believes they are likely not sufficient to maintain a lead over our competitors. That said, the Commission wants time to assess the Department's prioritization of AI across its R&D portfolio before making a specific recommendation for additional AI R&D funding for DoD.

Accordingly, the Commission focused its near-term attention on federal non-DoD R&D spending, which we considered a priority at this point in time. In subsequent memoranda, the Commission will provide actionable recommendations regarding the optimization of the DoD research enterprise for AI R&D, to enable strategic research investments and accelerate development and fielding of AI capabilities.

## ISSUE #1: AI R&D FUNDING LEVELS

In response to the Executive Order 13859, "Maintaining American Leadership in Artificial Intelligence," the Networking and Information Technology Research and Development (NITRD) Program adopted for the first time in 2019 a framework to capture AI R&D investments across the interagency.[11] This process defined $973M in requested FY 2020 federal investment in non-defense AI R&D.

Over the past five years, federal R&D funding for computer science (which houses AI) increased by 12.7 percent, barely sustaining a field in which tenure track positions at universities grew by 118 percent over the same period.[12] This mismatch has led to a plummeting acceptance rate of grant proposals, a scramble to fill open faculty positions, and an accelerating rate of academics departing universities for industry appointments. Illustrative of this situation is the fact that the core AI research budget of NSF's Computer and Information Science and Engineering (CISE) directorate is sufficient to meet only about half of the submitted AI research proposals rated as "competitive" and "highly competitive" through NSF's rigorous peer review process.[13]

In our interim report, NSCAI assessed the following**:**

- Current federal funding is not adequate to meet the growth of the field, let alone support its continued expansion.[14]
- Academic research is weakening as a result of the brain drain of professors and diversion of graduate students to industry.
- Steps must be taken to strengthen the talent pipeline for domestic students.

[11] In 2019, NITRD established an AI Program Component Area (PCA) and also asked agencies to capture AI-related research found in other PCAs. Using this framework, the FY 2020 federal AI R&D budget request came to $973M – $654M for direct AI investments and $319M in AI-involved investments captured in the other PCAs.

[12] See National Science Foundation (2018), https://www.nsf.gov/statistics/2019/nsf19321/#fig2; *Analysis of Current and Future Computer Science Needs via Advertised Faculty Searches for 2019*, CRA Bulletin (Dec. 7, 2019), https://cra.org/analysis-of-current-and-future-computer-science-needs-via-advertised-faculty-searches-for-2019/.

[13] In 2017, NSF funded $122M in core AI research, leaving $174M in highly rated proposals unfunded. In 2018, NSF was able to raise funding to $165M, but still left $185M in highly rated proposals unfunded.

[14] See NSCAI Interim Report at 24-28 (Nov. 2019), https://drive.google.com/file/d/153OrxnuGEjsUvlxWsFYauslwNeCEkvUb/view; *Analysis of Current and Future Computer Science Needs via Advertised Faculty Searches for 2019*, CRA Bulletin (Dec. 7, 2019), https://cra.org/analysis-of-current-and-future-computer-science-needs-via-advertised-faculty-searches-for-2019/.

- Application of AI to other fields of science and engineering holds the potential for significant return on investment.
- National technical and ethical standards for development are lagging behind the technology.

Should current trends remain unchecked, the United States' ability to train the next generation of AI talent, maintain the top global research institutions in AI, pursue the widest swath of fundamental research thrusts, and, ultimately, lead the world in cutting-edge AI research will degrade.

The President's FY 2021 Budget takes a step in the right direction for AI with additional investments in AI R&D through the NSF, DOE, National Institutes of Health (NIH), and the Department of Agriculture (USDA), and with a commitment to double funding for AI R&D by 2022.[15] Congress and the White House need to ensure the USG continues to fund research and development, as AI relies on advances in other fields such as mathematics, and much of the potential of the technology comes from its application across science and engineering fields.[16]

Preserving our leadership in AI and emerging technologies is a national security priority, as these technologies have the power to unlock new levels of economic prosperity, empower scientific and social advancements, reshape international norms, and underpin future national security capabilities.

## *Recommendation 1: Double non-Defense AI R&D Funding for FY 2021*

The Commission recommends that Congress roughly double the funding level of non-defense AI R&D for FY 2021 to begin to immediately address the funding deficit in the field and build the capacity for compounding higher levels of funding and investment in future years. **This funding should increase agency topline levels, not repurpose funds from within existing agency budgets, and be used by agencies to fund new research and initiatives, not to support re-labeled existing efforts.** We also recommend investments in specific fellowships administered by DoD and the Defense Advanced Research Projects Agency (DARPA), as well as in the national labs managed by DOE's National Nuclear Security Administration, which falls under the National Defense Budget. In Tab 4, we have also outlined recommended investments in DARPA's microelectronics program and recommend the establishment of a new microelectronics program in the Intelligence Advanced Research Projects Activity (IARPA), both with the goal of securing U.S. advantages in AI hardware.[17]

[15] Increased funding for AI R&D in the request encompasses $350M in additional funds for NSF to support AI research and establish AI Institutes, $54M additional for DOE's Office of Science, $100M additional for USDA, and $50M additional for NIH. The budget also allocates an additional $50M to NSF for workforce development initiatives around AI and QIS with a focus on community colleges, Historically Black Colleges and Universities, and Minority Serving Institutions. See The White House, *Advancing United States Leadership in the Industries of the Future*, https://www.whitehouse.gov/wp-content/uploads/2020/02/FY21-Fact-Sheet-IOTF.pdf. Note the detailed breakout of FY 2020 allocated and FY 2021 requested AI R&D investments by agency is not yet available, and will be released by OSTP in summer 2020. The Commission highlights the problematic timing of this information as counterproductive to informing the congressional appropriations process.

[16] If enacted, it would affect a nine percent drop in overall federal R&D funding, a decline of $13.78B. The FY 2021 request proposes reductions of 6 percent to NSF, 17 percent to DOE's Office of Science, 7 percent to NIH, 19 percent to NIST, and eliminates completely the DOE's Advanced Research Projects Agency - Energy.

[17] Note that these defense investments are not intended as topline increases, but to come from within existing defense budgets.

*Proposed Legislative Action*

The goal of this initial boost in funding is to meet the demonstrated need for resources across the AI R&D community in a manner that does not flood the environment, but leverages a variety of existing vehicles and pathways to strengthen basic and applied research, build talent, and bolster existing national research assets to embrace and apply AI. The Commission sees this as the first of several, successive increases to gradually build the nation's capabilities in AI research.

Given our understanding of the needs of the R&D environment and the strengths of various agencies, the Commission recommends investments in NSF, DOE, the National Institute for Standards and Technology (NIST), NIH, and the National Aeronautics and Space Administration (NASA); and an expansion of a range of existing fellowship vehicles to support students and faculty pursuing AI-related degrees and research. This approach provides a stimulus to strengthen AI in academia, deepen work at our national laboratories, and advance development across the broad network of government-sponsored and affiliated laboratories. It will support efforts to apply AI to federal agency missions, develop technical and ethical standards for AI technologies, expand AI across fields of science and medicine, build public-private partnerships, and demonstrate the positive potential of AI to the American people.

The Commission recommends that Congress increase AI funding by approximately $1 billion[18] and allocate the funding as follows:

- $450 million to NSF,[19] which is the preeminent science funding agency best poised to support the academic research community. These funds would support foundational AI research, research into semiconductors and microelectronics necessary for AI-related hardware,[20] and expand NSF's National AI Research Institutes Program and Cloudbank Program.[21]

- $300 million to DOE,[22] which oversees the nation's 17 national labs where a wide range of basic and applied research is conducted—in both open and classified environments. These national assets also host specialized high-performance computing and experimental facilities that can serve to accelerate the development of not only AI as a technology, but also novel hardware to support the evolution of AI and new AI-based applications critical to national mission areas. These labs also serve as valuable vehicles for public-private partnerships.

- $125 million to NIH, which has a proven track record of funding research transformational to U.S. public health and society. Opportunities include harnessing AI methods to address public health emergencies, such as the rise of new pathogens and

[18] See the Appendix for a detailed compilation of the Commission's initial funding recommendations. The Commission recommends topline increases for non-defense discretionary agencies (e.g., NSF, NIH, etc.) and reprioritization within the existing topline for national defense (050) agencies (e.g., DoD and NNSA).

[19] The recommended breakdown is $300 million to the CISE directorate for core AI research grants, $100 million to the National AI Research Institutes Program, and $50 million to semiconductor and microelectronics research.

[20] For more details on the proposed $50 million to semiconductors and microelectronics research, please see Tab 4, recommendation 2-3.

[21] See NSF, *National Artificial Intelligence Research Institutes*, https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=505686.

[22] The recommended breakdown is $150 million to DOE's Office of Science, $100 million to the National Nuclear Security Administration, $25 million to the AI and Technology Office, and $25 million to the Advanced Research Projects Agency - Energy.

pandemics, including applications in precision medicine for critical care, advanced therapeutics, logistics, and epidemiology. Additional funding for NIH efforts would expand efforts to apply AI to biomedicine and to neuroscience, which promise to have synergies with next generations of AI and AI-specific hardware, among other opportunities.[23]

- $50 million to NIST, which plays a critical role in developing standards with U.S. industry. These funds would enable NIST to lead the setting of protocols and nation-wide testing standards for AI, alleviating the cost burden from compliance with multiple standards at the local, state, and federal levels, and accelerating development and fielding of the technology. NIST would be able to expand its efforts to advance the tools to measure and understand the capabilities and limitations of AI technologies and its underlying data, building the confidence and trust needed to expedite technology adoption, deployment, and use.

- $75 million to NASA, to leverage its existing expertise in operational deployment of AI in space missions. Due to the urgent need for autonomous operations and AI in space domain[24] and the criticality of space to national security, we recommend this additional funding to enable NASA to expand its development and application of AI techniques tailored to the space domain and continue to serve as a pathfinder providing operational experience with AI. This work has direct applications to national security.[25]

- $100 million to expand select fellowship and scholarship programs managed by DoD, DOE, NASA, and NSF.[26] Additional funding through these vehicles would support additional undergraduate and graduate students to pursue AI-related fields of study, helping to strengthen academia, grow the domestic talent pipeline, and provide pathways into government for technical talent. Similarly, career/faculty fellowship vehicles supporting researchers in academia can serve to stem the flow of researchers to industry and invest in top talent to pursue big ideas.

The Commission recommends that Congress mandate reporting on the additional AI scholarships and fellowships awarded as a result of these increases.

[23] The Advisory Committee to the Director of NIH recently concluded a study on applying AI and machine learning to biomedicine, see NIH, *Artificial Intelligence Working Group Update: 119th Meeting of the Advisory Committee to the Director* (Dec. 13, 2019), https://www.acd.od.nih.gov/documents/presentations/12132019AI.pdf.

[24] AI for autonomous operations in space is critical due to requirements for fast response, limited communications and denied communications.

[25] Because other agencies indicated in this document experienced significant increases in FY20 in AI funding and NASA has not, we advocate a substantial proportional increase.

[26] Expanded at a standard rate of around 10 percent of FY 2020 enacted levels to incorporate more AI-specific awards in FY 2021. Programs include the following. For DoD: DARPA Young Faculty Award; Vannevar Bush Faculty Fellowship; Science, Mathematics, and Research for Transformation Scholarship for Service Program; National Defense Science and Engineering Graduate Fellowship Program; and Historically Black Colleges/Universities and Minority-Serving Institutions Research and Education Program. For DOE: Early Career Research Program; Computational Science Graduate Fellowship. For NASA: Space Technology Research Fellowship program. For NSF: CAREER fellowship; Graduate Research Fellowship Program; CyberCorps: Scholarship for Service; Historically Black Colleges and Universities Undergraduate Program; and Research Traineeship.

### *Recommendation 2: Prioritize Funding for Specific Areas of AI*

The Commission recommends that additional defense and non-defense AI research funding should be applied to advance six key areas in the field. In these areas, the Commission assesses that government support is critical to lay a foundation for our nation's future security.

The Commission recommends funding be prioritized for the following areas:

1. **Novel machine learning directions.** To further non-traditional approaches to supervised machine learning in an unsupervised or semi-supervised manner as well as the transfer of learning from one task or domain to another.

2. **Testing, Evaluation, Verification, and Validation (TEVV) of AI systems.** To develop a better understanding of how to conduct TEVV and build checks and balances into an AI system.

3. **Robust machine learning.** To cultivate more robust methods that can overcome adverse conditions, and advance approaches that enable assessment of types and levels of vulnerability and immunity.

4. **Complex multi-agent scenarios.** To advance the understanding of interacting AI systems, including the application of game theory to varied and complex scenarios, including interactions between cohorts composed of a mixture of humans and AI technologies.

5. **AI for modeling, simulation, and design.** To progress the use of rich simulations as a source of data and scenarios for training and testing AI systems, and to use AI to solve complex analytical problems and to serve as a generative design engine in scientific discovery and engineering.

6. **Advanced scene understanding.** To evolve perceptual models to incorporate multi-source and multi-modal information to support enhanced actionable awareness and insight across a range of complex, dynamic environments and scenarios.

This is by no means a comprehensive list, but rather an identification of near-term priorities in which government investment could have an outsized return on investment and advance the field toward future capabilities that will underwrite our national security and defense.

## ISSUE #2: AI R&D INFRASTRUCTURE

There is a growing divide in AI research between the "haves" in the private sector and the "have nots" in academia. Much of today's AI research depends on access to resource-intensive computation and large, curated data sets, both of which reside primarily in the private sector. Developing, maintaining, and executing compute capabilities needed to build a leading-edge model can cost from tens of thousands to hundreds of thousands of dollars, depending on the model and the end application. Access to open data on which to train such models is limited, which constrains the research initiatives of academics and students and skews projects towards existing data. Moreover, the expertise required to make effective use of these resources is not yet widely held, restricting progress to a limited number of institutions and fields.

This high-cost barrier to entry has hampered R&D in academia and benefited private sector efforts, limiting access to those outside of elite, well-funded institutions and weighting the nation's research portfolio toward applied, market-driven endeavors. This growing gap will degrade the long-term research and training functions performed by our nation's universities.

These limitations put transformative AI research efforts out of reach for most academic researchers, and limit the ability of universities to educate our next generation of AI practitioners. To fully harness the transformational nature of the technology, there is a need to democratize access to the resources that fuel the field.

Recognizing this, the Executive Order 13859 on AI called on federal agencies to "enhance access to high-quality Federal data, models, and computing resources to increase their value for AI R&D."[27] The White House's recently-released annual report on the American AI Initiative outlines that "it is the policy of the United States to expand the access of experts to high-quality, valid, and fully traceable Federal data, models, and computing resources for Federally funded AI R&D."[28] To this point, however, efforts to provide AI-ready government data to the research community have encountered barriers around data models, quality, discoverability, accessibility, as well as governance issues such as provenance, access constraints, privacy, safety, security, and intellectual property.

## *Recommendation 3: Launch a Task Force Study and Pilot Program to Establish a National AI Research Resource.*

To advance AI research in the United States, Congress should authorize and appropriate $25 million in funding for the first year of a five-year pilot program to develop, implement, and sustain a National AI Research Resource (NAIRR) infrastructure that would provide researchers and students with access to compute resources, co-located with AI-ready government data sets, educational tools, and user support.[29] This infrastructure would leverage public-private partnerships and build on existing government efforts, avoiding high start-up costs of a government-run data center.

The NAIRR pilot program would accelerate and strengthen AI research across the U.S. by removing the high-cost barrier to entry of compute resources while also fueling research and training through access to machine learning-ready data sets of real-world, representative U.S. government data.[30] Combined with the provision of training tools and support options, this infrastructure would democratize AI R&D outside of elite universities and big technology

[27] See The White House, *Executive Order on Maintaining American Leadership in Artificial Intelligence* (Feb. 11, 2019), https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.

[28] See The White House, OSTP, *American Artificial Intelligence Initiative: Year One Annual Report* at 9 (Feb. 2020), https://www.whitehouse.gov/wp-content/uploads/2020/02/American-AI-Initiative-One-Year-Annual-Report.pdf

[29] This program may be realized as a single cloud resource or a federation of resources, the pros and cons of which should be considered by the Task Force with determinations made within their resulting roadmap.

[30] This recommendation emphasizes U.S. government data within the NAIRR in order to facilitate and accelerate the sharing of government data sets; however, the NAIRR should also host non-government ML-ready data sets.

companies and further enable the application of AI approaches across scientific fields and disciplines, unlocking breakthroughs.[31]

*Proposed Legislative Action*

Congress should authorize a task force, co-led by NSF and the Office of Science and Technology Policy (OSTP), that includes representatives from key government agencies anticipated to contribute data sets to the NAIRR platform. The task force—composed of government leaders and representatives from the academic and commercial AI communities—would produce a roadmap laying out ownership, governance, capabilities, and sustainment of the national resource within 180 days of enactment. Once the roadmap is developed, funding for and implementation of a multi-year pilot would transition to the responsible agency determined through the study.

The roadmap would define the following:

- **Ownership**: Agency or organization responsible for the implementation, deployment, on-going development, and staff support for the NAIRR.

- **Governance**: Composition of the structural processes and oversight body needed to establish strategic direction, make programmatic decisions, and manage the allocation of resources. For example, defining the grant-making selection and allocation processes, selecting government and non-government AI-ready datasets to add to the NAIRR over time, and determining permissions and management of access to the data and resources hosted on the platform.

- **Capabilities**: Novel, scalable cloud architecture designed to enable secured access control; resident data engineering and curation expertise; provision of data sets that are findable, accessible, interoperable, and reusable; computation on hosted data that does not leave the platform; educational tools and services; and a user interface portal. The pilot implementation provides a proving ground for developing data interface and quality standards, curation best practices, anonymization techniques, and standardized procedures and criteria for determining which government and non-government data can be made publicly available under what conditions.

- **Sustainment**: Business model based in public-private partnerships that can support provision of scalable cloud resources and a staff of cloud architects, data engineers, and educational/technical support, all at a minimal cost to the researcher.

Funding for the pilot would support staffing of the program and the cloud resources (persistent data storage and compute services), augmented through public-private partnerships. Staff would be responsible for maintaining and improving the architecture solution, curating data sets, building interfaces and tools, and providing support to researchers as they use the NAIRR.

[31] For a similar proposal, see the recent call for establishing such AI research infrastructure by a consortium of 22 top U.S. universities, led by Stanford. John Etchemendy and Fei-Fei Li, *National Research Cloud: Ensuring the Continuation of American Innovation*, Human-Centered Artificial Intelligence, Stanford University (Mar. 29, 2020), https://hai.stanford.edu/news/national-research-cloud-ensuring-continuation-american-innovation

# 2. Recommendations to Accelerate AI Application in the Department of Defense

TAB 2

The Defense Department's efforts to develop, test, and deploy AI applications face obstacles throughout the adoption pipeline. These obstacles, many of which are structural impediments, currently prevent DoD from adopting AI-enabled technologies at the speed and scale required to maintain a competitive advantage over our near-peer competitors. They include: inadequate policy and governance structures, including unclear and misaligned authorities; insufficient infrastructure; and an antiquated and overly cumbersome acquisition system. While these obstacles are not unique to AI, they significantly inhibit progress on this critical emerging technology by preventing AI strategy from being effectively implemented, and by impeding technological breakthroughs in the lab and the private sector from translating into results in the field.

Individually, each of these challenges has been studied at length by past review teams, producing multiple reports and recommendations—many of which are just beginning to be implemented.[32] These efforts, while thorough, well-staffed, and well-intended, are constrained to making changes within the existing structures and oversight mechanisms that govern DoD. As a result, existing AI implementation efforts will likely create local efficiencies, but will not be able to create the necessary transformational change. The Department needs an integrated approach to AI that prioritizes and coordinates emerging technology across the life-cycle of research, development, and operational adoption; as well as an entity with accountability for the fielding of joint AI solutions.

The recommendations presented below are critical first steps to accelerate AI application in DoD. They focus on creating top-down leadership mechanisms that directly address three of the consensus judgements in the Commission's Interim Report: 1) that AI can help the United States execute core national security missions, if we let it; 2) that successful AI application is threatened by bureaucratic impediments and inertia; and 3) that top-down leadership is needed to overcome organizational barriers and create strategic change. These near-term recommendations should be implemented as soon as possible.

The Commission is continuing to develop longer-term recommendations that aim to fundamentally alter the Department's ability to apply enabling technologies and conduct continuous modernization. Going forward, the Commission will also study the technical application areas where AI can have the broadest and most significant impact across the Department. Ensuring DoD has the right posture to bring the right technology to bear is crucial to maintaining a competitive military advantage against future threats.

[32] Recent recommendations have come from the Defense Science Board, in "Design and Acquisition of Software for Defense Systems" (Feb. 2018); the Defense Innovation Board, in its "Software Acquisition and Practices Study" (Feb. 2019); the Section 809 Panel, in its report on "Streamlining and Codifying Acquisition Regulations"; and RAND, in its report, "The Department of Defense Posture for Artificial Intelligence Assessment and Recommendations" (2019). Some recommendations from those studies have led directly to reforms within DoD. The FY 2019 and FY 2020 National Defense Authorization Acts have also served as vehicles for implementing some of these recommendations.

## ISSUE #1: SENIOR LEADERSHIP REVIEW AND PRIORITIZATION OF EMERGING TECHNOLOGY

There is a long tradition of senior leaders across DoD and the Intelligence Community (IC) coming together to face global challenges. In the 1970s, Secretary of Defense Harold Brown and then Under Secretary of Defense Bill Perry led a coordination group that helped drive the development and fielding of revolutionary new systems, such as extended-range precision-guided munitions, stealth aircraft, and new intelligence, surveillance, and reconnaissance platforms. In 2014, DoD launched the Advanced Capabilities and Deterrence Panel (ACDP) to oversee the Defense Innovation Initiative, designed to identify and invest in innovative ways to sustain and advance U.S. technological and operational advantages against future threats. It was instrumental in the Department's pursuit of the Third Offset Strategy—an effort to generate a focused, deliberate institutional response to a changed strategic environment that created operational challenges that are very different than what the U.S. military had grown accustomed to in the post-Cold War era.

The ACDP was led by the Deputy Secretary of Defense, the Vice Chairman of the Joint Chiefs of Staff, and the Principal Deputy Director of National Intelligence. The ACDP monitored all aspects of the Defense Innovation Initiative, and provided oversight of all associated Departmental activities. Its key achievement was that it focused the Department's senior leadership on developing material and conceptual solutions to operational challenges facing the nation in high-end warfare against advanced adversaries. The ACDP integrated key leaders of the Department's components, services, and combatant commands and empowered them to adopt and employ new ideas outside the usual bureaucratic boundaries that limit speed and scale.

The ACDP was dissolved in 2018 after Department leadership determined that its lines of work should be subsumed within the broader project of implementing the new National Defense Strategy. However, as subsequent implementation of the strategy has shown, this type of high-level steering committee is necessary to drive change, focus, and action on emerging technology that otherwise would not be prioritized.

### *Recommendation 1: DoD and the Office of the Director of National Intelligence (ODNI) should establish a Steering Committee on Emerging Technology tri-chaired by the Deputy Secretary of Defense, the Vice Chairman of the Joint Chiefs of Staff, and the Principal Deputy Director of ODNI.*

Establishing such a tri-chaired committee will integrate DoD and IC AI efforts and provide the top-down focus needed for DoD to overcome the bureaucratic challenges impeding AI application. Specifically, it will help enhance intelligence analysis related to emerging technology, connect strategic vision to organizational change; focus concept and capability development on emerging threats; guide defense investments that ensure America's strategic advantage against near-peer competitors; and provide the authority to drive technology adoption and application by the Department. It will also make recommendations directly to the Secretary of Defense on Departmental innovation priorities.

*Proposed Executive Branch Action*

The Secretary of Defense and Director of National Intelligence should issue a directive immediately establishing the senior oversight committee described above. The Steering Committee provides a forum for the Office of the Secretary of Defense, the Joint Staff, and the Office of the Director for National Intelligence senior leadership to focus on developing concepts and capabilities that include emerging and disruptive technologies and meet current and future operational challenges facing the nation. Steering Committee members should include DoD and ODNI executives, including but not limited to the Chief Management Officer, appropriate Under Secretaries of Defense and Deputy Directors of National Intelligence, Office of the Secretary of Defense Office of Cost Assessment and Program Evaluation (CAPE), the Directors of the Joint Artificial Intelligence Center (JAIC) and the Augmenting Intelligence Using Machines Initiative (AIM), and the Vice Chiefs of the military services. The Under Secretary of Defense for Research and Engineering should provide technical expertise to the Committee, as aligned with their existing Departmental responsibilities. Service AI leads should participate when AI is the primary topic of discussion.

The Tri-Chaired Steering Committee should:

- Review credible assessments of emerging threats and identify adversary investments and advances in emerging technologies such as AI/ML, 5G, quantum computing, autonomy, robotics, bio-technology, nanotechnology, and other technologies as appropriate.

- Identify, prioritize, and resource technically and operationally feasible technology solutions to the most pressing operational challenges facing DoD as identified in the National Defense Strategy.
- Direct changes in existing programs as well as direct sufficient resources for experimentation and prototyping of one-off, high-risk, high-reward projects.

- Propose changes to existing policies and processes that are not optimized for today's non-linear, risk-taking technology innovation, which requires agility, creativity, and speed.

*Proposed Legislative Branch Action*

Congress should use the FY 2021 National Defense Authorization Act (NDAA) to establish the Tri-Chaired Steering Committee. While DoD and ODNI have the authority to establish such a forum without legislative action, codifying it into law will ensure that it is sustained through leadership transitions. The Commission recommends that such language remain sufficiently broad to enable flexibility in the Steering Committee's roles and responsibilities should they need to adapt as emerging technologies and Department efforts evolve.

## ISSUE #2: DEPARTMENT OF DEFENSE AI REPORTING LINES

As indicated in our Interim Report, pockets of successful bottom-up innovation across DoD are not translating into strategic change, and likely will not translate into such change without significant senior-level oversight and support. Like past technological changes, integrating AI will require top-down leadership and effective coordination to overcome cultural, policy, and process barriers to adoption. Establishing direct reporting authority to senior Department leadership would be in line with the designation of the JAIC Director as the Senior Official Responsible for AI within DoD and would reinforce AI as the Secretary of Defense's number one modernization priority.[33]

## *Recommendation 2: The Director of the Joint Artificial Intelligence Center (JAIC) should report directly to the Secretary of Defense, who may delegate this authority to the Deputy Secretary of Defense.*

This change ensures senior leadership oversight of DoD AI efforts and alignment with Department priorities by elevating JAIC's reporting authority, which currently runs through the Chief Information Officer (CIO), to the Secretary of Defense or his Deputy. This recommendation seeks to give the Secretary of Defense, or Deputy by delegation, the ability to exercise authority and direction over the JAIC. The Director of the JAIC should report directly to the Secretary of Defense or his Deputy regarding the JAIC's central roles and responsibilities. The JAIC's current organizational placement within the Office of the Secretary of Defense and its fiscal relationship to the Defense Information Systems Agency should remain unchanged. However, the JAIC and the CIO should fully separate in their roles and responsibilities. The JAIC should hold primary responsibility for AI applications, while the CIO should continue to lead DoD's broader digital transformation efforts.

Direct attention from senior leadership can drive organizational focus and empower coordinating entities to gain service support and move initiatives forward. Establishing Secretary of Defense authority and direction over the Department's leading AI effort provides the requisite level of senior oversight and support needed to preserve the Department's initial AI projects, enable their growth, and ensure the Department can develop the capabilities needed to successfully adopt AI applications.

A direct reporting line to senior leadership has precedent within the Department. The Strategic Capabilities Office (SCO), which also seeks to further defense innovation, was established in 2012. Since then it has held various reporting structures, including reporting directly to the Deputy Secretary. The direct reporting line gave SCO the visibility, support, and resources to build their capacity and prove their value to the services and to Congress. After organizational changes in recent years, Congress re-elevated SCO to report directly to the Deputy Secretary of Defense in the FY 2020 National Defense Authorization Act (Pub. Law 116-92, Sec. 233).

### *Proposed Executive Branch Action*

The Secretary of Defense should immediately issue a memo designating the Director of the Joint Artificial Intelligence Center as a direct report or delegate such authority to the Deputy Secretary of Defense.

[33] See Deputy Secretary of Defense Memorandum for the Chief Management Officer on the Designation of a Senior Official with Primary Responsibility for Artificial Intelligence (Oct. 2, 2019); and RAND, *The Department of Defense Posture for Artificial Intelligence* (2019), 8, https://www.rand.org/content/dam/rand/pubs/research_reports/RR4200/RR4229/RAND_RR4229.pdf; U.S. Senate, *Confirmation Hearing on the Nomination of Hon. Mark T. Esper to be Secretary of Defense* (July 16, 2019), 64, https://www.armed-services.senate.gov/imo/media/doc/19-59_07-16-19.pdf; Remarks by the Honorable Mark T. Esper, *NSCAI Conference on Strength Through Innovation* (Nov. 5, 2019).

Recommendations from the JAIC to the Secretary of Defense regarding new applications of, and modifications to, existing and near-term capabilities that provide an operational advantage to the Department should be reviewed by the new tri-chaired Steering Committee and, where appropriate, conveyed as investment recommendations to the Deputy's Management Action Group.

*Proposed Legislative Branch Action*

Congress should use the FY 2021 National Defense Authorization Act to establish the JAIC as a direct report to the Secretary of Defense, who may delegate this authority to the Deputy Secretary of Defense.

## ISSUE #3: REQUIREMENTS FOR THE DIRECTOR OF THE JAIC

The Department is currently deciding whether to maintain the current rank of the JAIC Director position at the level of a three-star general/flag officer or to shift to civilian leadership following the current director's planned retirement in summer 2020.

### *Recommendation 3: Maintain the Director of the JAIC as a three-star general or flag officer with proven operational experience.*

Three-star leadership allows the JAIC to engage with the services at a senior rank and within their command structure. Operational experience enables the Director to understand how AI can serve operational requirements and better communicate with the services as to how AI meets capability needs. This has helped the JAIC build inroads with the services as a new organization in the Office of the Secretary of Defense. Maintaining a strong relationship with the services is necessary going forward to enable the transition of AI applications to service programs as they become available and ensure application development meets service needs. Retaining this credibility is important in the short-term as the JAIC's programs and capabilities mature. However, the JAIC should retain the flexibility to consider changing to civilian leadership in the future and ensure strong AI technical expertise exists in supporting roles.

*Proposed Executive Branch Action*

The Secretary of Defense should require that the Director of the JAIC remain a three-star general or flag officer with significant operational experience.

*Proposed Legislative Branch Action*

Congress should use the FY 2021 National Defense Authorization Act to designate that the Director of the JAIC will be a three-star general or flag officer by creating a three-star billet for the role.

# 3. Recommendations to Strengthen the AI Workforce

TAB 3

Our defense and intelligence agencies need a workforce with expanded AI skills and expertise, including software engineers, data engineers and scientists, mathematicians, and machine learning experts. Their knowledge is required to buy, build, and use AI tools effectively. However, as we assessed in our Interim Report, the government has been slow to recognize the importance of these technical skills, and is struggling to attract, develop, organize, and retain an AI-ready workforce. These deficits make it difficult to implement AI solutions.[34]

The government does not have enough in-house expertise to quickly build an AI workforce. Doing so will also require the government to aggressively recruit talent from universities and the private sector to become government employees (or, when appropriate, contractors). Unfortunately, today's bureaucratic barriers make the government hiring and security clearance processes both difficult and time consuming, putting the government at a tremendous disadvantage. Technologists and many others often face a six month or longer hiring process, during which they may receive competing job offers, including some that would offer higher salaries than the government. For the government to compete in the AI job market, it needs to improve its hiring process for AI practitioners at all levels and across a wide array of agencies.

The government also should identify and develop the capabilities of its existing workforce. There are many current government employees who know how to develop AI technology, and others who have the potential to quickly learn how to do so. Unfortunately, the government does not have mechanisms in place to identify those individuals, or to incentivize their development. It is also true that for the government to successfully adopt AI, many if not most end users will need to gain a baseline understanding of AI's limitations, data management requirements, and ethical use.

This memorandum offers recommendations, divided into eight areas, that will start to address these problems: (1) the excepted service, (2) the role of human resource teams, (3) the effect of the security clearance process on hiring, (4) the use of resumes in the hiring process for AI practitioners, (5) developing end users' baseline understanding of AI, (6) identifying existing and potential talent, (7) building recruiting pipelines from universities into the government, and (8) improving talent exchanges between the government and private sector.

## ISSUE #1: THE EXCEPTED SERVICE

The U.S. government already has the vast majority of the authorities it needs to hire AI talent. Within the Department of Defense (DoD), however, current law ties some of those authorities too closely to cyber missions. While AI and cybersecurity are closely connected, they are not the same (see our discussion in the Interim Report, at footnote 117). AI can enhance a wide variety of operations and activities, including those outside the cyber domain. Combining the two workforces limits AI's application.

[34] NSCAI interview with U.S. government officials (May 24, 2019).

Currently, agencies with a critical need can shorten the standard government hiring process using authorities specific to STEM fields, especially direct hiring authorities and the excepted service. The Cyber Excepted Service (CES) in particular has shown success for specific commands such as Cyber Command and the Joint Artificial Intelligence Center, but its applicability to the DoD's AI workforce will be severely limited if it is not amended. CES can apply, by exception and by individual position, to a very limited number of AI-related positions within DoD. However, the section of Title 10 that establishes CES ties it to Cyber Command and positions within the military departments supporting Cyber Command.[35] As the AI workforce grows and becomes differentiated from the cyber workforce, many if not most AI positions will not be in support of Cyber Command, causing them to be excluded from the CES or face a prohibitively time consuming application process.[36]

## *Recommendation 1: Expand the Cyber Excepted Service*

The government should expand the CES to explicitly include AI positions, which should include positions that accomplish tasks described by Section 1051(f) of the John S. McCain National Defense Authorization Act of Fiscal Year 2019 (Pub. L. 115-232), which provides a working definition of AI for defense and national security purposes. Expanding the CES rather than creating a new hiring authority avoids contributing to the confusing proliferation of authorities and avoids delays from the time required to establish and begin using a new hiring authority. The government should also allow personnel hired under CES to be appointed to competitive service positions without competing as external, non-federal applicants.

It should be noted that cyber and AI are different fields. Expanding the CES to a Cyber and AI Excepted Service would avoid increasing administrative burdens and adding another hiring authority. This should not be taken as an indication that AI and cyber are synonymous, as the education and skills for each field differ. Also, the National Security Commission on AI believes the United States Government and Department of Defense may benefit from developing a digital corps, and is considering the steps needed to create one. The above recommendation is consistent with that end, and can be easily incorporated into a digital corps if the decision to pursue one is approved.

### *Proposed Executive Branch Action*

Extend the Defense Civilian Intelligence Personnel System Interchange Agreement (DCIPS IA) to personnel hired with the CES.[37] Current Title 5 employees that voluntarily transfer to CES will generally have Title 5 status. New hires often will not, damaging their ability to stay in government or move to other positions within the government that are outside the CES. This will impede the USG's ability to attract and retain talent. Extending the DCIPS IA will allow personnel hired under the CES to transfer to the competitive service with the same status as Title 5 employees.

[35] 10 U.S.C. § 1599f.

[36] NSCAI interview with a government official (Nov. 26, 2019).

[37] Defense Civilian Intelligence Personnel System, *Defense Civilian Intelligence Personnel System Interchange Agreement*, https://dcips.defense.gov/Portals/50/Documents/Fact%20Sheets/DCIPSFAQs_InterchangeAgreement_revised190625.pdf.

*Proposed Legislative Branch Action*

The Congress should use the National Defense Authorization Act to expand the CES to include AI positions. An expanded CES should allow the DoD and military services to hire AI practitioners more quickly. Hiring success metrics Congress should track should include: 1) how often the CES is used, 2) how often the CES is used for AI-related positions compared to the competitive service, 3) the number of job offers made using both the CES and the competitive service and their relative success rate, and 4) how quickly the DoD and military services hire AI practitioners compared to positions that do not have direct hiring authorities or excepted service.

Existing authorities for other national security departments and agencies are adequate as written, but not as widely used. Their challenge generally lies in receiving approval to use hiring authorities outside the competitive service. Organizations applying for excepted service status and direct hiring authorities from the Office of Personnel Management (OPM) frequently face barriers that either draw out the application process or prevent organizations from using processes outside of the competitive service.[38] Congress should require OPM to monitor the application process to evaluate the rate and speed at which exemptions to the competitive service are granted to applying agencies. OPM's reporting requirements to Congress should include: 1) the time required to complete the application process, 2) the percentage of applying agencies that complete the application process, 3) the percentage of applying organizations allowed to use the CES, and 4) the reason organizations are disapproved.

## ISSUE #2: THE ROLE OF HUMAN RESOURCE TEAMS

Human resource (HR) teams often struggle to correctly identify qualified personnel and use hiring authorities outside of the competitive service, preventing qualified candidates from joining the government and lengthening the hiring process for those who do.[39] Issues with HR teams are exacerbated by the prominent role they play in the hiring process. There are three groups involved in the hiring process, or what we refer to as the hiring triangle: HR, subject matter experts on the team with the open position, and organizational leaders. Today, a very large part of the discretion for government hiring lies with the HR team, experts play a smaller role, and organizational leaders are often less involved than would be ideal. This system is especially ineffective when hiring people whose resumes may inadequately capture their experience, or when HR experts do not have the niche knowledge needed to understand what the items on a resume mean.[40] This has resulted in instances where celebrated, world-class hackers, developers, and AI practitioners have been told they are underqualified to work at DoD, or can only enter at pay scales that significantly misrepresent their abilities compared to their peers in government.[41]

This is a marked contrast with private sector AI companies and traditional companies that have successfully integrated AI, which often consider their recruiting and talent management practices

[38] This refers both to Government-Wide Direct Hire Authority under 5 U.S.C. section 3304 and 5 CFR Part 337, subpart B, and to OPM delegated examining authority under 5 U.S.C. section 1104(a)(2) and (3).

[39] NSCAI interview with government officials representing multiple agencies (Sept. 9, 2019).

[40] The effectiveness of the use of the CES and other hiring authorities varies greatly among organizations within departments and agencies, leading to the conclusion that the hiring process is as dependent on HR teams' training, education, and intent as it is on department-wide infrastructure problems.

[41] The Defense Innovation Board has offered detailed recommendations on this topic. See https://innovation.defense.gov/.

a core part of their achievement. In these cases, human resource teams and hiring managers are closely tied to product development teams, understand the business and technical language in their field, and view their role as a core component of their teams' success.

## *Recommendation 2: Increase Human Resource Team AI Literacy*

The Department of Defense, Department of Homeland Security, Federal Bureau of Investigation, and Intelligence Community (IC) should establish a training and certification program for HR professionals that ensures:

- familiarity with their organization's goals regarding AI;
- hiring practices outside of the competitive service; and
- software development, AI, and AI workforce literacy for HR teams, hiring managers, and recruiters.

Agencies should audit short courses annually to ensure nomenclature, definitions, organization goals and vision, and other information maintains the accuracy and pace consistent with the evolution of AI.

### *Proposed Executive Branch Action*

The Department of Defense should establish short courses for HR professionals, hiring managers, and recruiters that are or will be responsible for hiring software developers, data scientists, or AI practitioners. The course should address applying for and the use of available hiring authorities, including but not limited to direct hiring authorities,[42] the Cyber Excepted Service,[43] special government employees, Intergovernmental Personnel Act, and highly qualified experts.[44] The course should also address the use of ePortfolio reviews (see below) and provide a general familiarity with the software development, data science, and AI fields. This includes an overview of software development and business processes, data management practices related to machine learning, an introduction to machine learning and deep learning, an introduction to AI, and AI workforce roles and archetypes.

### *Proposed Legislative Branch Action*

The Armed Services committees should use the FY 2021 NDAA to require the Department of Defense to establish a human resources software development, data science, and AI short course within one year of the NDAA's enactment. Twenty percent of the HR teams, hiring managers, and recruiters responsible for hiring software developers, data scientists, or AI practitioners should be required to pass the course by the end of the first year, with the minimum percentage certified increasing by ten percent each year until 80 percent of the applicable human resource workforce is certified. Equivalent practices are already the norm in some top-tier technology companies.[45]

[42] Office of Personnel Management, *Hiring Information: Direct Hire Authority*, https://www.opm.gov/policy-data-oversight/hiring-information/direct-hire-authority/#url=Governmentwide-Authority.

[43] Chief Information Officer, *Cyber Excepted Service (CES) Personnel System*, https://dodcio.defense.gov/Cyber-Workforce/CES.aspx.

[44] Office of Personnel Management, *Pay and Leave: Pay Administration*, https://www.opm.gov/policy-data-oversight/pay-leave/pay-administration/fact-sheets/expert-and-consultant-pay/.

[45] NSCAI interview with a private-sector company (July 12, 2019).

Appropriators should set aside $2.5 million of DoD O&M funding for the creation and execution of a short course for HR professionals, hiring managers, and recruiters.[46]

## Recommendation 3: Rebalance the Hiring Triangle

HR departments should not be in charge of selecting AI practitioners for the government workforce. Instead, qualified practitioners within the government workforce should be responsible for selecting their own team members, HR teams should be responsible for executing hiring processes with little discretion about hiring choices, and commanders and civilian leaders should aggressively assume more responsibility for the output of the entire process.[47] In addition, to reduce the burden placed on HR teams, subject matter experts should receive referral bonuses for civilian experts hired after applying based on the subject matter experts referral.

### *Proposed Executive Branch Action*

The Secretary of Defense should issue a memorandum of intent that rebalances the hiring triangle. The memorandum should include the following:

- A description of the flaws in the current hiring process for software developers, data scientists, and AI practitioners (see above);
- A mandate for commanders to assume greater responsibility for the results of civilian hiring of software developers, data scientists, and AI practitioners;
- Allow hiring managers to dictate the use of applicable direct hiring authorities, qualification standards, and to determine who is qualified;
- An increase in the role of subject matter experts such as software engineers in the hiring process;
- A reduction of the ability of HR professionals to determine if a potential employee is well qualified for software development, data science, or AI positions;
- A desire to use direct hiring authorities and the Cyber Excepted Service when they are the fastest way to hire qualified personnel; and,
- A requirement to report the status of software engineer and AI practitioner hiring in the organization, including hiring time, use of hiring authorities besides the competitive service, and the role of subject matter experts in hiring decisions.

### *Proposed Legislative Branch Action*

The Armed Services committees should use the FY 2021 NDAA to require the Department of Defense to provide referral bonuses to software development, data science, and AI experts. DoD Instruction 1400.24-V451 already authorizes the use of referral bonuses for recruitment and hiring, but it is unclear how often it is used and to what effect. Performance metrics should include the number of times performance bonuses are awarded per year, both in gross numbers and as a percentage of hiring decisions for positions involving software development, data science, and AI. Performance metrics should also include hiring time and the use of hiring authorities besides the competitive service.

[46] One to two-day introduction to AI courses from competitive companies frequently cost between $500 and $1,000.

[47] Commanders and civilian leaders should hold their HR teams and subject matter experts accountable for hiring timelines and the quality of new hires, but should not be required to be directly involved in screening resumes.

Appropriators should set aside $100,000 of O&M funding for each military service and for the Office of the Secretary of Defense to use as referral bonuses for software development, data science, and AI experts.

## *Recommendation 4: Grant Exemption from OPM General Schedule Qualification Policies for Specific Billets and Position Descriptions*

Even when subject matter experts are able to choose their applicants, they are constrained by OPM minimum qualification standards. While these are important and have increased fairness in hiring, they also prevent expert technologists that do not have master's degrees, and in some cases bachelor's degrees or comparable work experience, from joining the government at a reasonable level of compensation. For example, a 19 year-old software developer or AI practitioner might have a proven track record on cybersecurity or in AI competitions, but can only enter the government as a GS-7. To reduce this hiring challenge, the government should allow agencies to exempt certain billets from OPM general schedule qualification policies, and instead allow local hiring managers to make an independent decision about both hiring and the pay grade.

### *Proposed Executive Branch Action*

Two-star and above commands and their civilian equivalents should be authorized to declare individual billets and position descriptions exempt from OPM qualification standards without approval from OPM or any more senior authority within the DoD. Separately, OPM should create and execute a process by which federal departments and agencies can apply for billets or position descriptions to be exempt from general schedule qualification policies. Once the process has been created, it should be integrated into Human Resource Team AI Literacy training (see above).

### *Proposed Legislative Branch Action*

Authorizing committees should direct the Office of Personnel Management to amend 5 CFR § 338.301, on service appointments, to allow service secretaries and cabinet officials to create exceptions from the Qualification Standards for General Schedule Positions by individual billet or position description.

## ISSUE #3: THE EFFECT OF THE SECURITY CLEARANCE PROCESS ON HIRING

One reason national security departments and agencies have not been able to recruit the technical talent they need to accomplish their AI goals is the length of time required to receive a security clearance. As a result, AI practitioners hired by the government often face long wait times before they can start work. During this waiting period, some early career practitioners instead choose to enter the private sector, where they can begin working and accessing data and models far more quickly. Later career practitioners, already in the private sector, may also therefore choose to stay there, rather than explore options in the government.

The Office of Personnel Management and the Defense Counterintelligence Security Agency (DCSA) have reduced the investigation backlog.[48] It is unclear, however, if ongoing security clearance reforms will be adequate to significantly improve AI recruitment issues. The DCSA plans to reduce the time required for a top secret clearance to 80 days and for a secret clearance to 40 days.[49] While that would be a significant improvement, an 80-day wait time may still put the government at a distinct disadvantage compared to private sector employers, particularly companies that are hiring high-demand AI practitioners. These changes also will not resolve long wait times for clearance adjudication, which now delays clearances more than investigations.[50]

## *Recommendation 5: Accelerate Security Clearance Investigation and Adjudication*

The USG should allow leaders of two-star and above commands and their civilian equivalents to prioritize personnel hired under the CES and for AI, data science, and software development positions during the security clearance process, and set a standard that they have an interim secret clearance within 20 days and an interim top secret clearance within 30 days. Prioritizing Cyber Excepted Service hires will be contentious, as almost every organization believes its subject matter experts or leaders should be a high priority. There is a strong case that AI genuinely and uniquely requires prioritized security clearances. First, due to the small number of AI practitioners both in the United States and around the world and the degree of skill it requires, AI is a uniquely talent-dependent field. Second, the commercial and academic demand for AI practitioners is extremely high and competitive. AI practitioners that put their work on hold for months at a time to wait for a security clearance can, and sometimes do, simply turn to the private sector and are quickly hired at a salary the government cannot match. Third, senior leaders, including the Secretary of Defense[51] and the Principal Deputy Director of National Intelligence,[52] have made AI their leading technology priority, but their departments and agencies have been unable to hire the talent they need to implement AI. These reasons support the argument that AI-related positions are genuinely a higher priority for security clearances than other positions.

### *Proposed Executive Branch Action*

Upon request by a two-star and above commands or their civilian equivalents, the Defense Counterintelligence and Security Agency should accelerate the security clearance process for personnel being hired under the Cyber Excepted Service and for AI, data science, and software development positions, and set a standard that they have an interim top secret clearance within 30 days and an interim secret clearance within 20 days of receipt of the SF86. The process can be established with a separate, parallel infrastructure to other security clearances, or by prioritizing personnel hired under the Cyber Excepted Service.

[48] Lindy Kyzer, *OPM Cuts Security Clearance Backlog in Half, But Processing Delays Spell Trouble for Pentagon*, Government Executive (July 22, 2019), https://www.govexec.com/management/2019/07/opm-cuts-security-clearance-backlog-half-processing-delays-spell-trouble-pentagon/158586/.

[49] Todd Lopez, *DOD to Take Over Background Checks by Fiscal 2020*, Defense News (June 25, 2019), https://www.defense.gov/explore/story/Article/1886923/dod-to-take-over-background-checks-by-fiscal-2020/.

[50] Lindy Kyzer, *Why is Your Clearance Still Delayed But the Investigation is Over*, Clearance Jobs (March 18, 2019), https://news.clearancejobs.com/2019/03/18/why-is-your-clearance-still-delayed-but-the-investigation-is-over/.

[51] Jane Edwards, *DOD Nominee Mark Esper Cites AI as Top Modernization Priority*, ExecutiveGov (July 17, 2019), https://www.executivegov.com/2019/07/dod-nominee-mark-esper-cites-ai-as-top-modernization-priority/.

[52] Jack Corrigan, Spy Agencies Turn to AI to Stay Ahead of Adversaries, NextGov (June 27, 2019), https://www.nextgov.com/emerging-tech/2019/06/spy-agencies-turn-ai-stay-ahead-adversaries/158081/

*Proposed Legislative Branch Action*

The Armed Services committees should use the FY 2021 NDAA to require the DCSA to establish an accelerated security clearance timeline for personnel being hired under the Cyber Excepted Service and for AI, data science, and software development positions as defined in the John S. McCain National Defense Authorization Act of Fiscal Year 2019 (P.L. 115-232). The time required for these personnel to receive interim secret and top secret clearances should be included as a quarterly briefing or reporting requirement to the Armed Services committees.

## *Recommendation 6: Create Unclassified Workspaces*

National security departments and agencies need to establish facilities where employees waiting on security clearances can perform unclassified work until they receive a clearance. This will allow organizations to quickly hire new employees, even when their security clearance process takes longer.

*Proposed Executive Branch Action*

The Secretary of Defense, Secretary of Homeland Security, and Director of National Intelligence should issue guidance directing their respective organizations to establish, within 180 days of publication, unclassified work spaces for AI practitioners at major commands, combatant commands, and major research facilities within 180 days of publication.

*Proposed Legislative Branch Action*

The Armed Services committees should use the FY 2021 NDAA to require the DoD, Department of Homeland Security (DHS), and IC to create unclassified workspaces for uncleared AI practitioners at major commands, combatant commands, and major research facilities.

## ISSUE #4: THE USE OF RESUMES DURING THE HIRING PROCESS FOR AI PRACTITIONERS

National security departments and agencies struggle to effectively identify qualified personnel based on resume reviews, the primary mechanism for screening applicants for most government positions. It is difficult to identify qualified AI workers based purely on the academic credentials shown on most resumes. Carnegie Mellon University offers a degree in AI, but many other schools with consistently top-ranked AI programs in the United States, such as University of Washington and the Massachusetts Institute of Technology, do not.[53] At other universities, and even at universities with AI programs, graduates with academic training in AI most commonly study computer science, mathematics, physics, neuroscience, psychology, and philosophy. Only a fraction of the people that study these subjects, however, graduate with formal credentials in AI that would be easily recognized in a resume screen. While a growing number of programs offer degrees in AI, it is unclear if they will become the primary source of academic AI expertise.

In addition, because AI and software development are sometimes self-taught fields, top-tier experts do not always have resumes that effectively convey their expertise. This is especially true

[53] Carnegie Mellon University, *B.S. in Artificial Intelligence*, https://www.cs.cmu.edu/bs-in-artificial-intelligence.

when those reviewing resumes are not familiar with software development and AI.[54] This includes world-class AI experts that do not have undergraduate or graduate degrees at all. Human resource teams have rejected well-known experts in their fields due to their lack of formal or recognizable qualifications, often during the initial screening process or even after internal government experts have acknowledged the applicant's expertise. In some cases, senior leaders have intervened; in other cases, the experts withdrew their applications.[55]

## *Recommendation 7: Use ePortfolio Reviews*

When hiring AI practitioners, the Department of Defense, Department of Homeland Security, and Intelligence Community should use resumes for their initial screening process, then during the remainder of the evaluation process replace resume reviews with an ePortfolio review designed to evaluate data science, software development, and AI competency. This approach would be based on private sector best practices both at major software companies and at small start-ups.[56] ePortfolio reviews show examples of an applicant's previous development work as a tangible demonstration of his or her capabilities.[57] To minimize applicant requirements and screener workload, an ePortfolio should contain three examples of the applicant's best work. This recommendation is closely linked to the above recommendations that address the role of HR teams. If SMEs do not assume a larger role in the hiring process and HR teams and hiring managers are not trained to read an ePortfolio, the process will be ineffective and potentially harmful. To implement this change, the Department of Defense should pilot the use of ePortfolio reviews in a major office or command.

### *Proposed Executive Branch Action*

The Department of Defense, Department of Homeland Security, and Intelligence Community should develop and implement an ePortfolio review process for software development, data science, and AI positions and invite applicants to submit ePortfolios. All ePortfolio review teams must have subject matter experts with skill sets related to the open position leading the review process. HR professionals who are involved in ePortfolio reviews should receive training on both topics.

### *Proposed Legislative Branch Action*

The Armed Services committees should use the FY 2021 NDAA to mandate the piloting of ePortfolio reviews in at least one major office or command. The pilot should be evaluated based on successful and unsuccessful applicant's perception of the application process and existing employee's perception of the effectiveness of the piloted ePortfolio review process. If the pilot has positive results, Congress should direct national security departments and agencies to review and update policies that inhibit the broad application of ePortfolio reviews rather than resumes during the hiring of technologists within one year of the completion of the pilot.

[54] NSCAI interview with a government official (Sept. 9, 2019).

[55] J. Michael McQuade, Richard Murray, Gilman Louie, Milo Medin, Jennifer Pahlka, and Trae' Stephens, *Software is Never Done: Refactoring the Acquisition Code for Competitive Advantage*, Defense Innovation Board, DoD (May 3, 2019), 57-58.

[56] NSCAI interviews with government and private sector personnel (June 4, 2019, July 12, 2019, and Aug. 9, 2019).

[57] Ross Miller and Wende Morgaine, *The Benefit of E-portfolios for Students and Faculty in Their Own Words*, Association of American Colleges & Universities, Winter 2009, Vol. 11, No. 1, https://www.aacu.org/publications-research/periodicals/benefits-e-portfolios-students-and-faculty-their-own-words.

## ISSUE #5: DEVELOPING END USERS' BASELINE UNDERSTANDING OF ARTIFICIAL INTELLIGENCE

National security departments and agencies need to improve AI literacy at all ranks and in many roles. An AI literate workforce understands the basics of the application of AI, computational thinking, hardware, and where appropriate, foundational concepts of data science. Many government employees are not familiar with AI at all, and receive the majority of their information from media representations of AI that often overstate AI capabilities or portray unrealistic scenarios of out of control AI systems. The NSCAI staff has interviewed numerous government officials from different departments and at different levels of seniority who will freely admit they do not understand basic AI concepts. Government organizations have done little to show their employees that AI literacy is valued, either by tracking proficiency, creating opportunities for training, or by rewarding demonstrations of competence.

The lack of AI literacy is particularly challenging within the DoD because of the high stakes and large scale involved in AI adoption. Data-centric AI involves many end users effectively updating and managing data sets. Doing so requires training and is more likely to take place when end users have an understanding of what the data sets will be used for and why they are important. This is particularly true for DoD applications, such as predictive maintenance and personnel management. If the government does not increase baseline AI and data management literacy, it will struggle to adopt and use AI, leading to missed opportunities, unnecessarily inefficient processes, and diminished readiness.

The goal is to improve baseline AI literacy by introducing AI to the entire workforce, not to build a small cadre of experts or to train acquisition and contracting professionals how to purchase AI solutions, important tasks that will be addressed in later recommendations. Deep expertise is necessary, and should be identified where it exists.[58] But it is also helpful to improve the entire workforce's understanding of AI's potential and limitations, use of AI-enabled systems, management of data sets, and ability to work with developers and experts who build and update AI capabilities.

## *Recommendation 8: Mandatory AI Training*

DoD and DHS should require mandatory training designed to improve baseline AI literacy, either online or in person. The training should focus on end users and their ability to collect and manage data, and include a short introduction to AI with an emphasis on machine learning, data management, the capabilities and limitations of AI, software decision-making, probabilistic reasoning, and an introduction to the responsible and ethical development and fielding of AI.[59] Ideally, these requirements should be integrated into existing user training programs rather

[58] Developing and managing AI experts will be addressed in later sets of recommendations.

[59] Among other things, mandatory training is intended to teach end users to implement better data collection and management practices, and to direct that behavior towards enabling the development of better AI. Because of the nature of their work and their lack of AI education opportunities otherwise, mandatory training is likely to help DoD and DHS. This is less true for the IC, which already has better educational opportunities, and the FBI, which doesn't have as many people involved in data collection and management. That is also why the IC, FBI, and other agencies are included in certified self-development.

creating new, separate training requirements. Annual AI training should be mandatory for five years, followed by an assessment of the need to continue the training.

There is well-justified resistance to increasing mandatory training. The Army recently reduced its mandatory training requirements based on the belief that they distracted from combat-focused training, damaging readiness.[60] While that is accurate for many mandatory training requirements in the past, it will not be the case for well-executed AI training. AI, if implemented successfully, will help organizations become more efficient and effective, and create new capabilities. DoD and DHS currently struggle to implement AI solutions due to a lack of baseline knowledge, which, as described above, is a greater challenge to readiness than the requirement to conduct an annual training course.

### *Proposed Executive Branch Action*

DoD and DHS should evaluate current commercial offerings for AI courses and determine the best fit based on their organizations' needs. The course should be structured with successive levels of comprehension, annual repetitions, and certification for different levels of competency. The course should include baseline instruction in the nature, development, limitations, and application of AI and data science and the basics of data management. Instruction related to the responsible and ethical development and fielding of AI should also be included (see Tab 6, Recommendation 1). Both departments should also establish and implement a system for tracking course completion and compensating those who complete the course.

### *Proposed Legislative Branch Action*

Authorizing committees should mandate that the DoD and DHS develop and implement mandatory annual training to improve AI literacy. For mandatory annual training, authorizing language should mandate course implementation, annual course assessment and revision, the development of course completion tracking, and the establishment of compensatory time-off for course completion within 180 days of legislation being signed into law, and that departments and agencies notify the respective committees when this has been accomplished.

Appropriators should set aside $20 million in DoD defense-wide O&M funding and add $20 million to DHS's topline to establish and execute AI mandatory annual training.

## *Recommendation 9: Certified Self-Development*

The government should reward and track employees that successfully complete certified AI training and courses. While mandatory training can require government employees to complete courses aimed at providing a minimum baseline knowledge of AI, it will also benefit the government to encourage employees to voluntarily extend their AI literacy beyond those minimum requirements. A broad array of online courses in data science, data engineering, and AI are readily available to meet individual interests, abilities, and goals (for example, Coursera and Udemy both offer free courses that come from leading experts and universities). Completion of

[60] Office of the Secretary of the Army, *Army Secretary Releases Reduction Requirement Memos to Improve Readiness* (June 15, 2018), https://www.army.mil/article/207160/army_secretary_releases_reduction_requirement_memos_to_improve_readiness.

these courses builds familiarity and skills directly related to adopting, integrating, and using AI capabilities inside the government (see Tab 6, Recommendation 1).

Rewards can take several forms. Employees can receive reimbursement for course tuition and fees, akin to existing education benefit programs within the Armed Services. Bonuses can be paid for course completion, as is done with special military skill designations or proven proficiency in a foreign language. For enlisted service members, points towards promotion can be added, similar to how other resident or non-resident course completions are factored into promotion competitions within some services. Likewise, additional time-off awards can be granted to employees, beyond their normal time accrual, for course completions. Course completions should be documented and taken into account when making assignments.

There is a legitimate concern that the government might approve online courses of limited technical or educational quality. To avoid this issue, organizations should seek out educational programs from successful AI companies that already offer public or internal education and training and R1 universities (doctoral universities with very high research activity).

*Proposed Executive Branch Action*

The DoD, DHS, Department of State (DoS), Department of Commerce (DoC) Bureau of Industry and Security, Federal Bureau of Investigation, and IC should develop a list of approved online courses related to AI. Lists should include at least one course addressing the ethical and responsible use of AI. Funding should come through the Department or Agency's centralized training or personnel office to allow individuals to directly access funded courses to maximize access. The organizations should authorize a 72-hour pass for uniformed service members who complete online courses, and authorize their use stand-alone or in conjunction with leave, holiday, or weekend periods. They should also authorize eight hours of leave for civilian employees who complete online courses. Both passes and leave should be authorized once per fiscal year quarter. Within the DoD, the Undersecretary of Defense for Personnel Readiness should be responsible for providing guidance on the above recommendations, including the development of an approved list of courses and funding sources.

*Proposed Legislative Branch Action*

For certified self-development online courses, authorizing language should mandate that the Secretaries of Defense, Homeland Security, State, and Commerce, and the FBI Director, and the Director of National Intelligence each publish a list of approved courses that shall be assessed and revised annually, funding mechanisms, and an incentive system within 120 days of legislation passing, and notification of authorizing committees when the first uniformed service members and civilian full-time employees have begun and completed online courses.

Appropriators should set aside $20 million in DoD Personnel funding to establish and execute certified self-development AI online courses and to compensate employees for successful completion. DHS and ODNI should also receive $20 million in total funding each for AI course development and employee compensation. Appropriators should set aside $5 million each to the DoS, DoC, and FBI to establish and execute certified self-development AI online courses and to compensate employees for successful completion.

## ISSUE #6: IDENTIFYING EXISTING AND POTENTIAL TALENT WITHIN THE GOVERNMENT

Government employees who can code enable experimentation and adaptation in daily operations, which can unlock unexpected capabilities and accelerate modernization. Personnel who have the capacity and the drive to learn to code are of value to the government's efforts to use AI—just as relevant foreign language skills are vital in counter-insurgency, intelligence collection, and diplomatic missions overseas. There are already a number of AI practitioners and data scientists within the government, and an even larger number of government employees with the ability to code. Most are identified only by reputation or word of mouth, not by any identifier that career managers or personnel offices can view.[61] While parts of the government are moving to resolve this issue, these efforts are not widespread enough and are moving too slowly.

The government's struggle to identify its existing software development, data science, and AI talent makes it difficult for career managers to fill positions that require existing skill sets. It also reduces the incentives for individuals to pursue self-development. Likewise, the government's struggle to identify potential talent hampers its ability to effectively choose individuals for further training and investment.

### *Recommendation 10: Measure and Incentivize Programming Proficiency*

The government needs a systematic way to identify employees with existing AI-related skills so that it can put people in the best position to make significant contributions. To do so, the government should measure and incentivize its employees' computer programming proficiency. Programming proficiency can be incentivized through various means. As with foreign language proficiency, bonuses can be paid for different, quantified levels of comprehension and skill. Programming proficiency should also be documented and taken into account when making assignments.

Notably, programming ability is only necessary for part of the AI workforce. Many AI practitioners who focus on algorithm development and the use of existing AI frameworks have minimal programming ability, but are still experts in their field. We recognize that measuring and incentivizing programming ability will improve the government's software development and some components of the AI lifecycle, but will not be a complete solution on its own.

#### *Proposed Executive Branch Action*

The DoD, DHS, IC, and FBI should create tests comparable to the Defense Language Proficiency Test (DLPT) that include coding languages and a second test for AI competency, and expand their use to non-DoD organizations. The DLPT evaluates and scores proficiency on select languages. Service members are given financial rewards for scoring sufficiently high ratings in valued languages. Proficiency is also tracked in service members' personnel files.[62] Departments and agencies should reassess the test annually to ensure that it remains up to date with commercial practices. Within the DoD, the Under Secretary of Defense for Personnel and Readiness should

[61] NSCAI interviews with several government officials (May 17, 2019 and June 6, 2019).

[62] Defense Language Institute Foreign Language Center, *DLPT Guides & Information*, https://www.dliflc.edu/resources/dlpt-guides/.

be responsible for a coding language testing and incentive pay program for service members. The Defense Civilian Personnel Advisory Service should be responsible for extending the program to civilian personnel, including tracking proficiency with the Defense Civilian Personnel Data System.

### *Proposed Legislative Branch Action*

Authorizing committees should mandate the development and implementation of an annually reassessed coding language proficiency test and an AI competency test within the DoD, DHS, IC, and FBI. The Armed Services committees should use the FY2021 NDAA to direct that testing and incentive pay be available within the DoD, and for DoD to coordinate with the IC, and DHS within a year of each bill's passage into law.

Appropriate $3 million in DoD O&M funding for the development and implementation of a coding proficiency test. Appropriators should set aside $1.25 million per service and $500,000 for the Office of the Secretary of Defense for coding language incentive pay.

## *Recommendation 11: Adjust the ASVAB to Identify Computational Thinking*

The government needs a systematic way to identify potential talent so that it can avoid wasting training resources or putting personnel in positions where they are unlikely to succeed. DoD should adjust the Armed Services Vocational Aptitude Battery Test (ASVAB) to measure computational thinking. We consider computational thinking to include "the thought processes involved in formulating problems and their potential solutions in ways that the solution can be effectively carried out by an information-processing agent (human or machine, or more generally, by a combination of both). More colloquially, [computational thinking] encompasses a set of processes that defines a problem, breaks it down into components, and develops models to solve the problem, then evaluates the result, iterates changes, and does it again."[63] Once adjusted, the test should be made available to civilian employees who are interested in voluntarily demonstrating aptitude for additional training.

The last major revision of the standardized test was in 2002 (the year most people entering the military in 2020 were born) and mostly involved administrative changes. The test can be updated again to identify computational thinking skills relevant to the military application and operation of information systems, computer language, data science, data engineering, and AI. This includes problem decomposition, abstraction, pattern recognition, analytical ability, the identification of variables involved in data representation, as well as the ability to create algorithms and solution expressions.

### *Proposed Executive Branch Action*

The Under Secretary of Defense for Personnel and Readiness should oversee adjustments to the ASVAB to measure computational thinking. Results should be used to place personnel in career

[63] Committee on STEM Education of the National Science & Technology Council, *Chartering a Course for Success: America's Strategy for STEM Education* at 23 (Dec. 2018), https://www.whitehouse.gov/wp-content/uploads/2018/12/STEM-Education-Strategic-Plan-2018.pdf.

fields and to identify personnel for further training, similar to the manner in which the Defense Language Aptitude Battery is used.

### *Proposed Legislative Branch Action*

The House and Senate Armed Services committees should use the FY 2021 NDAA to mandate that the Under Secretary of Defense for Personnel and Readiness research and draft a new portion within the ASVAB that identifies and measures computational thinking based on existing academic and private sector testing, with language directing that the addition be incorporated into ASVAB testing a year after the bill is signed into law.

## ISSUE #7: BUILDING RECRUITMENT PIPELINES

The U.S. government struggles to hire recent college graduates, especially those with AI-relevant skills.[64] Many have little exposure to the personal and societal benefits of government service, especially when compared to their exposure to the private sector. They are instead left with what are often negative narratives about government employment. If students look past those narratives, they still have to overcome barriers created by a complicated, drawn-out hiring process. All three factors create a gulf between technically skilled graduates and their government.[65] The result is a government workforce with twice as many workers over 60 as under 30 years old that struggles to modernize, and a student population that typically chooses private sector work over government service.[66]

To overcome these obstacles, national security departments and agencies need to create hiring pipelines that accomplish the following:

- Expose college students to interesting government work,
- Demonstrate the benefits and opportunities found in government work,
- Initiate the hiring process before students commit to other employers and early enough that students can work immediately after graduation, including in work that requires a security clearance,
- Serve as a screening process for potential permanent employees, and
- Incentivize government service.

[64] Office of Personnel Management, *Hiring Information: Students & Recent Graduates*, https://www.opm.gov/policy-data-oversight/hiring-information/students-recent-graduates/.

[65] Amy Zegart and Kevin Childs, *The Divide Between Silicon Valley and Washington Is a National-Security Threat*, The Atlantic (Dec. 13, 2018), https://www.theatlantic.com/ideas/archive/2018/12/growing-gulf-between-silicon-valley-and-washington/577963/.

[66] Courtney Buble, *The Aging Federal Workforce Needs 'New Blood,' Experts Say*, Government Executive (Aug. 30, 2019), https://www.govexec.com/workforce/2019/08/aging-federal-workforce-needs-new-blood-experts-say/159585/.

## *Recommendation 12: Create Opportunities for Students to be Exposed to Government Work by Hiring University Professors as Part-Time Government Researchers*

To create opportunities to interact with students, some private sector companies hire university faculty as summer or part-time researchers. The companies benefit from access to a diverse group of experts that understands and often creates the world's most cutting-edge AI. In turn the companies provide resources, exposure to new techniques, and financial compensation to the professors, sometimes including funding for their university-based lab. When the professors return to teaching, they also expose promising students to the companies' work, creating student awareness and excitement about the available opportunities, a positive perception of the companies, and relationships that encourage student employment upon graduation.

To replicate this proven technique, the Department of Energy (DoE), DoD, DoC, DHS, and IC should hire university faculty with relevant STEM expertise to serve as part-time researchers in government laboratories. Faculty members could work during sabbaticals, summer breaks, or limited hours throughout the year.

Some government laboratories already hire university professors as part-time researchers. It is unclear how often this happens, the return on investment when it takes place, or how often faculty expose their students to government work, internships, or employment. These metrics should be tracked and, if helpful, the programs should expand and specifically include faculty with expertise in AI.

### *Proposed Executive Branch Action*

The DoE, DoD, IC, DHS, and DoC should establish STEM professor recruitment programs that include:

- Outreach to and recruitment at universities, conferences, and professional organizations.
- The creation of at least ten part-time researcher billets, five of which are specifically for AI researchers, at laboratories and research facilities including but not limited to the Los Alamos National Laboratory, Oak Ridge National Laboratory, Lawrence Livermore National Laboratory, Army Research Laboratory, Air Force Research Laboratory, Naval Research Laboratory, and the National Security Agency Laboratory for Advanced Cybersecurity Research. Each lab should have the authorization to recruit, screen, select, and compensate part-time professors at the laboratory's local leadership's discretion, not through a centralized hiring mechanism at the agency level.
- It should be noted that 10 HQEs is a minimum, and laboratories should not interpret the above guidance as a constraint on any other outreach programs or methods for working with faculty.
- Specified authorization for research facilities in the program to use direct hiring authorities and pay in 10 U.S.C. § 1599h. Under section 1599h, the laboratories of the military departments, DARPA, and Director of Operational Test and Evaluation have the authority to hire experts in science and engineering under their own program of personnel management authority. This authority exempts authorized programs from some sections of title 5 that address hiring processes and terms of employment, including allowing for 150 percent of the vice-president's salary in financial compensation in a

single fiscal year. This would allow organizations that fall under section 1599h to hire professors in part time capacities at a competitive salary.

- Specific authorization for research facilities to hire experts, consultants, and highly qualified experts outside of the competitive service system. Section 3109 of Title 5 authorizes agencies to hire experts whose education and experience allows them to perform tasks beyond the range of a competent person in that field and consultants that can provide valuable and pertinent advice. Both types of employee can serve up to one year or on an intermittent basis, and their base pay rate cannot exceed that of a GS-15 step 10's hourly rate.[67] Another section of Title 5 authorizes the DoD to hire up to 2,500 highly qualified experts for up to five years, with an additional year at the Secretary of Defense's discretion.[68]
- A referral bonus for other faculty hired under the part-time faculty researcher program and interns who participate in laboratory internship programs and the Pathways Internship Program.
- Expand the use of Cooperative R&D Agreements (CRADAs) between government organizations, universities, and the private sector to enable joint research and expertise sharing.[69]

*Proposed Legislative Branch Action*

Authorizing committees should mandate that the DoE, DoD, DoC, DHS, and IC begin programs to hire university faculty with relevant STEM expertise as part time researchers at Los Alamos National Laboratory, Oak Ridge National Laboratory, Lawrence Livermore National Laboratory, Army Research Laboratory, Air Force Research Laboratory, Naval Research Laboratory, National Security Agency Laboratory for Advanced Cybersecurity Research, and other laboratories at their discretion within 180 days of the passage of legislation. Performance measures include:

- the number of faculty hired within 365 days of the passage of legislation;
- after two years, the number of college interns and recently graduates interviewed and/or hired after a reference from faculty part-time researchers each year; and
- the results of faculty part-time researchers work after two years.

Appropriators should set aside such sums as necessary for the DoE to hire 10 university professors as part-time researchers at each DoE laboratory, up to a total of 170 professors, and to award recruitment bonuses. Appropriators should set aside such sums as necessary for the DoD to hire 10 university professors as part-time researchers at each DoD laboratory, up to 100 professors, and to award recruitment bonuses. Appropriators should set aside such sums as necessary for the IC to hire 10 university professors as part-time researchers at each IC laboratory, up to a total of 30 professors, and to award recruitment bonuses. Appropriators should appropriate such sums as necessary for the DoC to hire 10 university professors as part-time researchers at each DoC laboratory, up to a total of 30 professors, and to award recruitment bonuses.

[67] Office of Personnel Management, *Pay & Leave: Pay Administration*, *Graduates*, https://www.opm.gov/policy-data-oversight/pay-leave/pay-administration/fact-sheets/expert-and-consultant-pay/.
[68] 5 U.S.C. § 9903.
[69] U.S. Naval Research Laboratory: Technology Transfer Office, *Frequently Asked Questions*, https://www.nrl.navy.mil/techtransfer/FAQs/CRADA.

## *Recommendation 13: Increase the Use and Utility of Pathways Internships*

The government should increase the use of the Pathways Internship Program as a mechanism to screen and hire new employees. Many government organizations already use internships as a hiring pipeline. Effective internship programs allow agencies to vet candidates, begin the security clearance process early enough for students to receive a clearance prior to graduation, establish relationships with students before they commit to another employer, and to expose students to the benefits of government work.[70]

Three major challenges currently reduce the Pathways Internship Program's effectiveness as a hiring mechanism. The first is a cap on the number of qualified applicants. Today, some government internship program application windows are only open for minutes before they reach the limit on the number of applications and close. This prevents well-qualified applicants from participating in the program. National security departments and agencies should eliminate such caps on the number of applicants.

The second challenge is the OPM Qualification Standards. Federal regulations allow individuals to "be evaluated against either agency-developed standards or the OPM Qualification Standard for the position being filled."[71] Many agencies default to the generic OPM standards[72] rather than creating their own, position-specific standards. Government agencies should create their own, position-specific qualification standards for internship positions.

The third challenge is the difficulty many Pathways Interns face when trying to convert to a full-time, competitive service position upon completion of their educational requirements. Currently, internships may be converted to a permanent position within 120 days of completing the program if they have completed 640 hours, completed their degree, meet the position's qualifications and requirements, and perform their job successfully.[73] This structure makes it difficult for students to convert a summer internship into a full-time position the following year.

*Proposed Executive Branch Action*

The Office of Personnel Management (OPM) should expand the Pathways Internship Program. National security departments and agencies should increase their student recruitment efforts, with a focus on recruiting undergraduate and graduate students with computer science, mathematics, electrical engineering, and computer engineering majors.

Departments and agencies participating in the Pathways Internship Program should eliminate the application cap and be required to develop their own position-specific qualification standards for Pathways Internship positions.

[70] NSCAI interview with government officials (June 24, 2019).
[71] 5 CFR § 362.203(c).
[72] Office of Personnel Management, *Group Coverage Qualification Standard for Schedule D, Pathways Internship Position,* https://www.opm.gov/policy-data-oversight/classification-qualifications/general-schedule-qualification-standards/final-groupcoveragequalificationstandardforpathwaysprogramschedule-20d.pdf.
[73] Office of Personnel Management, *Hiring Information: Students & Recent Graduates*, https://www.opm.gov/policy-data-oversight/hiring-information/students-recent-graduates/#url=intern.

OPM should change the requirements for computer science, mathematics, electrical engineering, and computer engineering majors to allow conversion within 365 days of completing a program, and after completing 220 hours of work. This will allow students who complete an internship the summer between their junior and senior years to initiate the security clearance process, complete their senior year, and convert to a full-time position after graduation.

*Proposed Legislative Branch Action*

Authorizing committees should require the DoD, IC, DoS, DoC, DHS, and Department of Justice to increase the number of Pathways Internships and the number of conversions to full-time positions, including for mathematics and computer science majors, within 365 days of the passage of legislation.

Authorizing committees should direct the Office of Personnel Management to change 5 CFR § 362.203(c) to read: "Qualifications. Individuals will be evaluated against agency-developed standards."

Authorizing committees should direct the Office of Personnel Management to change 5 CFR § 362.204(b)(1) to read: "Completed 220 hours of work experience acquired through the internship program, except as provided in paragraphs (c) and (d) of this section, while enrolled as a full-time or part-time, degree- or certificate-seeking student."

Authorizing committees should direct the Office of Personnel Management to change 5 CFR § 362.204(b)(2) to read: "Completed a course of academic study, within the 365-day period preceding the appointment, at a qualifying educational institution conferring a diploma, certificate, or degree."

Performance metrics Congress should monitor include:

- The change in the number of Pathways Internship Program participants from the three previous fiscal years to the current fiscal year,
- The change in the number of mathematics and computer science majors participating in the Pathways Internship Program from the three previous fiscal years to the current fiscal year,
- The change in and overall number of conversions from the Pathways Internship Program to full-time positions from the three previous fiscal years to the current fiscal year, and
- The change in the number of mathematics and computer science majors who convert from the Pathways Internship Program to full-time positions from the three previous fiscal years to the current fiscal year.

## Recommendation 14: Expand the CyberCorps: Scholarship for Service

The Office of Personnel Management and National Science Foundation should expand the scope of CyberCorps: Scholarship for Service (SFS). The CyberCorps SFS is a recruiting program designed to attract students studying IT, cybersecurity, and related fields into the USG. Expanding it could bring in more people with AI-related skills. It is managed by the National Science Foundation in partnership with the Office of Personnel Management and the Department of Homeland Security. Students enrolled in the program receive a scholarship in exchange for an obligation to work in an approved government agency for a period of time equal to the time covered by the scholarship. Seventy undergraduate and graduate institutions participate in SFS by selecting students for the program, and since 2001, 3,600 students have received scholarships, 94 percent of whom went on to serve in government. Hiring typically takes place during annual online and in-person career fairs.[74]

It should be noted that cyber and AI are different fields. Expanding CyberCorps: SFS to CyberCorps and AI: SFS would avoid increasing administrative burdens. This should not be taken as an indication that AI and cyber are synonymous, as the education and skills for each field differ. Also, the National Security Commission on AI believes the United States Government and Department of Defense may benefit from developing a digital corps, and is considering the steps needed to create one. The above recommendation is consistent with that end, and can be easily incorporated into a digital corps if the decision to pursue one is approved.

### *Proposed Executive Branch Action*

The National Science Foundation and Office of Personnel Management should broaden the CyberCorps: SFS to pay for up to four years and to include fields falling under digital engineering, as those fields are defined by the National Defense Authorization Act for Fiscal Year 2020 (Pub. L. 116-92, section 230): "the discipline and set of skills involved in the creation, processing, transmission, integration, and storage of digital data, including data science, machine learning, software engineering, software product management, and artificial intelligence product management."

### *Proposed Legislative Branch Action*

The Armed Services committees should broaden the CyberCorps: SFS to include digital engineers, as defined by section 230 of the National Defense Authorization Act for Fiscal Year 2020, to pay for up to four years of scholarships, and to include the opportunity to begin the security clearance process.

The Armed Services committees should amend 15 U.S.C. § 7442 subsection (a) to read: "...recruit and train the next generation of information technology professionals, digital engineers, artificial intelligence practitioners, data engineers, data analysts, data scientists, industrial control system security professionals, security managers, and cybersecurity course instructors to meet the needs of the cybersecurity mission for Federal, State, local, tribal, and territorial governments."[75]

The Armed Services committees should amend 15 U.S.C. § 7442 subsection (b) to provide an opportunity for scholarship recipients to initiate their security clearance process at least one year before their planned graduation date.

The Armed Services committees should amend 15 U.S.C. § 7442 subsection (c) to allow the scholarship to last for 4 years.

[74] Office of Personnel Management, *Start Your Cybersecurity Career with the U.S. government*, https://www.sfs.opm.gov/.

## ISSUE #8: IMPROVING TALENT EXCHANGES

The bulk of innovation, development, and integration of AI applications is being driven by the private sector. Presently, however, there are few opportunities for government personnel to pursue hands-on exposure to what is being done to develop and adopt AI in the private sector, or for private sector employees to temporarily serve in government. In part, this is due to the nature of careers within the armed forces and civilian national security institutions, which justifiably require iterative training and continual rotation of assignments directly related to specific career fields and do not foster or incentivize experiences outside the government.

U.S. law and DoD directives both provide some allowances for public-private talent exchange and government employee training with industry. Under 10 U.S.C. § 1599g, the Secretary of Defense may, with the agreement of a private-sector organization and the consent of the employee, arrange for the temporary assignment of the employee to that private-sector organization. This legislation is the foundation for the Department of Defense Talent Exchange policy published in July 2018, as is the 2016 Department of Defense Instruction 1322.06, which sets out the procedure for Defense personnel to accept fellowships and exchange tours with corporations. These programs are an opportunity for personnel to learn how to create AI enterprise strategies, understand the software development process, and gain technical skills. Of particular note are the Secretary of Defense Executive Fellows program,[76] the Undersecretary of Defense for Acquisition and Sustainment's Public-Private Talent Exchange program,[77] and the Air Force Education with Industry program.[78]

The relatively few available opportunities are spread across the whole of the commercial sector and not specifically aimed at addressing the government workforce competency and experience gap with AI. They are also not being used as a component of the education, training, and professional development for military and civilian personnel to learn from AI development, testing, adoption, and integration in the private sector. More can be done to harness and expand this existing vehicle to answer the shortfalls that exist within the national security establishment with respect to AI experience and expertise.

[76] For the past 16 years, the Secretary of Defense Executive Fellows program has placed military officers and civilian leaders inside commercial enterprises to expose them to strategy, operations, finance, and logistics practices in the private sector. Each Service has historically selected annually between two-to-five officers plus Service civilians in management ranks. Companies that have sponsored the year-long program include 3M, Accenture, Amazon, Amgen, Apple, Boeing, Booz Allen, Caterpillar, Cisco, DuPont, ExxonMobil, FedEx, General Dynamics, Google, Honeywell, Hewlett-Packard, Intel JPMorgan Chase, Lockheed Martin, Merck, Microsoft, Morgan Stanley, Northrop Grumman, Oracle, Raytheon, Salesforce.com, SAP, Shell, Southern Company, SpaceX, Union Pacific, and United Technologies. This program is trea

[77] The Undersecretary of Defense for Acquisition and Sustainment is sponsoring the second class of the Defense Department's Public-Private Talent Exchange program. The program cohort includes five mid-career Defense Department civilian employees selected for a six-month tour in industry, and five employees of a private-sector organization selected to work in the DoD for the same period. The program is focused on the DoD's acquisition workforce and acquisition-related issues. The aim is to advance the DoD's understanding of industry's business operations and innovation best practices—and industry's comprehension of the same in government. Government participants are in residence with defense sector corporations such as Boeing, Booz Allen Hamilton, Deloitte, General Dynamics, Guidehouse, Northrop Grumman, and Raytheon.

[78] Since 1947, the U.S. Air Force has conducted an Education with Industry program. Approximately sixty Air Force officers, enlisted, and civilians are selected each year for the ten-month fellowship. Program fellows today are primarily personnel with seven-to-fourteen years of service, that is captains and majors, staff sergeants through master sergeants, and civilians GS-11 through GS-13; all from a variety of different career fields. An example of the range of companies participating in the program includes Amazon, Microsoft, Boeing, and Blue Origin.

## *Recommendation 15: Increase the Number of Fellowships and Partnerships with Industry, and Increase the Number Focused on Artificial Intelligence and Software Development*

National security departments and agencies should increase the number of fellowships and partnerships with industry, particularly fellowships with AI and software companies. The number of fellows, particularly from the DoD, needs to increase significantly if service members and civilian employees are to garner and leverage the AI-related experience and expertise resident in the private sector. Moreover, individual participation in these fellowships should be treated, for the purposes of promotion boards and subsequent assignments, as having an experience equivalent to graduating from a resident professional military education program.

Notably, this is not a recommendation to shift the focus of fellowships and partnerships with industry away from other fields, many of which add significant value to the government. Instead, the number of government and private sector employees participating in fellowships and partnerships with industry should significantly increase, with many of the increased number going to or coming from AI and software companies.

*Proposed Executive Branch Actions*

- **Secretary of Defense Executive Fellow Program:** The Office of the Secretary of Defense should expand the Secretary of Defense Executive Fellow Program. In addition to previous nomination requirements, each service and the Office of the Secretary of Defense should be required to nominate an additional eight uniformed service members or government civilians for sponsorship by major corporations that are leading in AI applications.

- **Public-Private Talent Exchange Program:** The Undersecretary of Defense for Acquisition and Sustainment's Public-Private Talent Exchange Program should both expand and increase its partnership with AI focused companies. Without changing the private sector partners of the current five employee cohort, the Undersecretary of Defense for Acquisition and Sustainment should grow the program by ten government employees who work with AI companies and ten private sector participants from AI focused companies. The Undersecretary of Defense for Research and Engineering, Department of Defense Chief Information Officer, military service secretariats, and Office of the Director of National Intelligence should establish similar AI-centric, 20-person talent exchange programs.

- **USAF Education with Industry Program:** The Air Force's Education with Industry Program should be replicated by the other military services and the IC, but with a focus on private sector companies working on AI applications. Likewise, participation in these programs should be treated, for the purposes of promotion boards and subsequent assignments, as equivalent to attending resident professional military education.

- **Public-Private Exchange Program Billet Office:** DoD should establish a Public Private Exchange Program Billet Office whose primary purpose is to temporarily hold billets for civilian DoD participants in exchange programs, roughly comparable to student detachments for active-duty personnel attending joint professional military education programs. Currently, DoD employing offices are disincentivized from encouraging employees to participate in exchange programs, as they lose a member of their team for an extended period, often without a replacement due to the strictness of the billeting process.[79] A Public Private Exchange Program Billet Office can reduce this disincentive by holding temporary billets for employees that participate in exchange programs, allowing employing offices to temporarily backfill their loss. To avoid the creation of yet another disincentive, employees who participate in talent exchange programs should be guaranteed that their previous position will remain available, even if it is temporarily filled while they participate in the exchange program.

### *Proposed Legislative Branch Action*

Authorizing committees should amend 10 U.S.C. § 1599g to direct the DoD and Office of the Director of National Intelligence to exchange talent and promote training with the commercial tech sector working on AI applications. Section 1599g should also reflect minimum participation requirements for talent exchange programs, as outlined above. The Office of the Secretary of Defense, military service secretaries, and Office of the Director of National Intelligence should provide an annual report to the authorizing committees about the status of their talent exchange programs.

[79] Advisory Panel on Streamlining and Codifying Acquisition Regulations, *Report of the Advisory Panel on Streamlining and Codifying Acquisition Regulations*, https://discover.dtic.mil/wp-content/uploads/809-Panel-2019/Volume3/Recommendation_61.pdf.

# 4. Recommendations to Promote U.S. Leadership in AI Hardware & 5G

## TAB 4

Advanced AI algorithms rely on high-end compute capabilities and the infrastructure to move large amounts of data at high speeds. As the Commission's Interim Report describes in detail, U.S. leadership in microelectronics is essential for leadership in AI, and the United States has enjoyed strategic advantages in microelectronics since the field's inception in the mid-twentieth century. However, this lead is currently eroding, and the risk to the safety and security of the U.S. semiconductor supply chain is increasing.[80]

To maintain leadership and ensure that the U.S. government (USG) adopts AI for national security applications successfully, the United States must take two steps simultaneously. First, it must invest in pathways for government access to state-of-the-art (SOTA) trusted microelectronics. Achieving trusted microelectronics requires scaling quantitative assurance with limited impacts on performance, developing a domestic fabrication facility featuring a trusted chain of custody over components and intellectual property, joint ventures with commercial firms, or a combination of approaches. Second, it must invest sustained R&D in future microelectronics technologies which will facilitate continued increases in performance despite the slowdown of Moore's Law scaling.[81] However, access and R&D must also be coupled with improved USG pathways for transitioning IP into and out of government applications. Although not covered here, commercial transition strategies will be a subject of future Commission study.

The following recommendations include discrete actions that Congress and the Executive Branch can take in the near term through FY 2020 reprogramming actions and the FY 2021 appropriations and authorization processes. These initial recommendations lay the groundwork for long-term access to resilient, trusted, and assured microelectronics for AI advantage, and will help ensure that the United States continues running faster than potential adversaries in the field of cutting-edge microelectronics.

This tab also provides limited, near-term recommendations to bolster U.S. fifth-generation wireless communications (5G) capabilities, recognizing that secure 5G infrastructure will be necessary to form the connective tissue between AI systems. Given the urgent need to create global 5G alternatives to Huawei, the Commission is providing select, immediate options for early consideration.

[80] See the Appendix at the end of this Tab for additional information on microelectronics global market trends, as well as explanations of some key terms and concepts.

[81] Moore's Law states that the number of transistors on a chip, and by extension its capability, will double every two years, a prediction which has largely held true since 1975. However, transistors can only physically be so small; a single atom of silicon is 0.2nm in diameter, and the manufacturing process of leading chips has a minimum distance of 5nm – or 25 atoms wide. As companies approach the anatomical limit of transistor size, they will have to find other ways to innovate in order to improve performance – such as potentially utilizing photons rather than electrons to transmit information – which may slow the iterative improvement process and cause Moore's Law to end.

# ISSUE #1: LACK OF ACCESS TO SECURE, ADVANCED MICROELECTRONICS FOR AI

The United States lacks domestic facilities capable of producing, integrating, assembling, and testing SOTA microelectronics at scale. This includes trusted and assured multi-chip packages (MCP), which are critical for national security applications. This lack of access forces the USG, as well as the U.S. defense industrial base and other commercial U.S. firms, to rely on foreign fabrication and complex global supply chains for production, which increases risks to product integrity and exposes U.S.-developed intellectual property (IP) to theft. According to a DoD official, this gap should provoke a "graceful and considered kind of panic" among U.S. policymakers.[82] For economic competitiveness and national security, the USG needs access to trustworthy high-performance microelectronic components across commodity, custom, semi-custom, and hybrid categories.[83]

## *Recommendation 1: Expand USG AI-Enabling Microelectronics Programs*

Expand USG access to high-performance, secure microelectronic components by developing novel and resilient sources for producing, integrating, assembling, and testing AI-enabling microelectronics.

*Proposed Funding Actions*

### *Recommendation 1-1: Expand the Navy led, DoD-wide existing advanced packaging, assembly and testing technical execution area under the Trusted and Assured Microelectronics Program that is led by the Office of the Under Secretary of Defense for Research and Engineering. Create a trusted state-of-the-art AI hardware demonstration prototype for multi-chip packages (AI-MCP) by reprogramming $50 million in FY 2020 or appropriating $50 million in FY 2021.*

In FY 2020, DoD is pursuing public-private partnerships under its Trusted and Assured Microelectronics Program to develop heterogeneous integration and advanced packaging of microelectronics in a secure U.S. manufacturing facility. The existing program does not include an AI specific application prototype demonstrator. This recommendation would expand the program to incorporate AI-specific capabilities for reduced size, weight, and power (SWaP), with increased performance and IP protection necessary for forward deployed DoD weapon system applications.

[82] Don Clark, *Pentagon, with an Eye on China, Pushes for Help from American Tech*, New York Times (Oct. 25, 2019), https://www.nytimes.com/2019/10/25/technology/pentagon-taiwan-tsmc-chipmaker.html; National Defense Industries Association, Trusted Microelectronics Joint Working Group, *New Methods to Instill Trust in Commercial Semiconductor Fabrication* (July 2017), https://www.ndia.org/-/media/sites/ndia/divisions/working-groups/tmjwg-documents/ndia-tm-jwg-team-4-white-paper-finalv3.ashx?la=en.

[83] Dr. Lisa Porter, *The U.S. Defense Department's New Thinking on Microelectronics Security*, Department of Defense (2019), https://science.dodlive.mil/2019/09/10/the-defense-departments-new-thinking-on-microelectronics-security/; National Academies of Sciences, Engineering, and Medicine, AS USAF, *The Growing Threat to Air Force Mission-Critical Electronics* at 1 (2019), https://www.nap.edu/catalog/25475/the-growing-threat-to-air-force-mission-critical-electronics-lethality.

As part of the Trusted and Assured Microelectronics program, Naval Surface Warfare Center Crane (NSWC Crane) initiated a SOTA Heterogeneous Integrated Packaging (SHIP) prototype program utilizing an Other Transaction Authority (OTA) agreement with a U.S.-based global leader in microelectronics in FY 2020.[84] With an additional $50 million, SHIP could expand the existing pilot prototype program to include heterogeneous integration of multi-chip packages incorporating AI specific chips and configurations. SOTA digital processing chips could include Field Programmable Gate Arrays (FPGAs), Application Specific Integrated Circuits (ASICs), or Graphics Processing Units (GPUs) tightly coupled with memory and leading edge, high-speed communications chips to reduce processing latency and also include "root-of-trust" security features to protect IP. SHIP would partner with one or more defense industrial base partners in conjunction with DoD program offices that would be responsible for transitioning and fielding the AI-MCP capability once successfully demonstrated.

A successful pilot program would also allow any DoD component—and potentially any USG organization—to purchase the AI-enabled microelectronics MCP using the same contract vehicle. This funding could be reprogrammed in FY 2020 or included in DoD's FY 2021 appropriation. Without the additional $50 million in FY 2021 funding, AI-centric capabilities will not be included in the pilot prototype program, delaying the development of heterogeneously integrated AI-specific microelectronics capabilities indefinitely.

### *Recommendation 1-2: Fund an accelerated site survey by the Office of the Director of National Intelligence for a U.S.-based commercial front-end-of-line semiconductor manufacturing facility by reprogramming funding in FY 2020 funding or by appropriating funding in FY 2021.*

The ability to reliably source trusted state-of-the-art microelectronic components is critical for United States commercial companies and for current and future USG national security capabilities. At present, the USG does not have trusted access to SOTA microelectronics manufacturing. Numerous studies conducted by or on behalf of the U.S. government have highlighted this issue and offered recommendations, including work by the Institute for Defense Analysis, the National Academy of Sciences, and DoD's Office of Military Industrial Base Policy, among others.[85] However, many well-founded recommendations have not been adopted and the

[84] The current plans for SHIP will provide DoD, other government agencies, and U.S. contractors assured access to a U.S. facility capable of integrating best-of-breed, state-of-the-art advanced-node MCPs. Heterogeneous integration allows DoD to combine the best SOTA commercial-off-the-shelf (COTS) integrated circuits (e.g., FPGA, processor, memory, analog-to-digital converters, and very high-speed input/output) with specialized government-off-the-shelf (GOTS) integrated circuits in a single MCP, optimized for DoD applications. The program also supports further customization by enabling a secure design flow for the creation of DoD specific integrated circuits (chiplets for integration in MCP), leveraging advancements in Electronic Design Automation (EDA) tools to expedite circuit design and transition technologies that offer DoD programs of record an asymmetrical advantage. The SHIP program's goals include achieving initial production capability by FY 2022 with the capacity to scale to 100,000 MCPs per month by FY 2025. Under the existing program, the initial prototype pilots will demonstrate capability for advanced radar and Electronic Warfare (EW) applications, and begin reliability and qualification activities for more specialty applications including radiation hardening for space and strategic systems.

[85] Interagency Task Force in Fulfillment of Executive Order 13806, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States* (Sept. 2018), https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF; Daniel J. Radack et. al., *Semiconductor Industrial Base Focus Study – Final Report*, Institute for Defense Analyses (Dec. 2016), https://www.ida.org/-/media/feature/publications/s/se/semiconductor-industrial-base-focus-study--final-report/d-8294.ashx; National Academies of Sciences, Engineering, and Medicine, *The Growing Threat to Air Force*

challenge has only compounded with time. For economic competitiveness and national security, the USG must act swiftly to meet the challenge of assured access to SOTA microelectronics manufacturing while simultaneously protecting sensitive IP and ensuring that manufactured parts operate only as intended.

The Office of the Director of National Intelligence has assessed opportunities to partner with U.S.-owned private-sector semiconductor companies to establish a SOTA semiconductor design, fabrication, and packaging facility in the United States that would meet USG technical and security needs for high-end semiconductors and help achieve cutting-edge performance levels. This capability would complement DoD's SHIP program. While building a cutting-edge, high-capacity semiconductor fabrication plant for dedicated-government use would likely cost approximately $20 billion, the ODNI approach calls for a security-based split-manufacturing facility and partnering with a private sector firm to build a facility, which would produce both commercial-use and government-use chips. The Front-End-of-Line (FEOL) portion—also known as circuit building blocks—could be produced within the standard commercial areas of the facility, along with standard commercial chips. For chips that will be used for controlled but unclassified, export-controlled, or classified uses, the Back-End-of-Line (interconnects and circuit function) layers could be produced on a separate government-certified secure line either in the same facility or at a separate facility, to which access could be controlled. The final assembly, packaging, and testing would also occur in a secure facility. This arrangement provides additional supply chain integrity and protects sensitive USG IP.[86]

The site survey is an essential first step toward moving forward with this project. This step can be funded and started immediately, would provide a specific cost of the overall project within 12-18 months, and could have the effect of lowering the overall estimated cost of the facility. The FY 2021 President's Budget request for microelectronics does not include funding for this site survey. Adding funding for the survey in FY 2021 would ensure that facility construction could proceed as quickly and efficiently as possible, should the USG decide to move forward with this recommendation.

### *Recommendation 1-3: Continue fully funding DoD's Trusted and Assured Microelectronics Program in the FY 2021 Budget.*

In the FY 2021 President's Budget, DoD's Trusted and Assured Microelectronics research, development, test, and evaluation (RDT&E) request includes $489 million for advanced component development and prototypes (ACD&P) and $108 million for system development

*Mission-Critical Electronics* (2019), https://www.nap.edu/catalog/25475/the-growing-threat-to-air-force-mission-critical-electronics-lethality.

[86] This approach offers several advantages relative to relying on offshore facilities for SOTA microelectronics. First and foremost, it would allow the United States to tailor high-end chipsets to boutique needs and use cases, giving it the ability to create cutting-edge ASICs (Application Specific Integrated Circuits) or FPGAs (Field Programmable Gate Arrays) optimized for running AI algorithms for national security missions, which has the potential to provide significant performance advantages over off-the-shelf chipsets. Second, this approach ensures that chipsets used within sensitive U.S. systems and networks have not been tampered with or compromised, as the United States would have end-to-end control over their domestic production, and would ensure the protection of chip design IP. Third, the split-manufacturing approach would cost significantly less than a SOTA USG-only facility, as the private sector firm would share a significant proportion of the costs, and both the USG and the private sector firm would benefit from economies of scale. ODNI estimates that the facility would have substantial longevity, and would be capable of filling USG needs for fabrication of exquisite and high-end chipsets through the mid-to-late 2030s.

and demonstration (SDD).[87] Combined, these programs will improve access to advanced packaging and testing; support the development of quantifiable assurance and secure design; develop foundry access standards; expand access to non-complementary metal oxide semiconductor (CMOS) SOTA microelectronics; support disruptive research and development; and promote education and workforce development. These are foundational microelectronics capabilities that will also enable the development and application of AI/ML capabilities across national security mission areas. Congress has fully funded the Administration's request for the DoD Trusted and Assured Microelectronics Program in each of the past three years. This recommendation endorses the Administration's request for Trusted and Assured Microelectronics in FY 2021.

*Proposed Executive Branch Actions*

### *Recommendation 1-4: OUSD/R&E should develop clear metrics for transitioning AI-enabling microelectronics from research programs to operating forces and the commercial sector.*

Despite successful research efforts to advance the fields of microelectronics and AI, pathways for transitioning advanced capabilities to the battlefield remain challenging. AI-specific microelectronics could accelerate the performance of machine learning capabilities across DoD mission areas, but only if they can be manufactured at scale. At the same time, more intellectual property generated through DoD research programs could be transitioned to the commercial sector to further spur innovation.

As a first step toward these goals, DoD should clarify its approach and plans for transitioning research efforts on advanced microelectronics to battlefield advantage through existing programs of record. It should also identify metrics for transitioning intellectual property it does not need to exclusively retain to enable further research and development outside the government, especially in the commercial sector.

This recommendation urges USD R&E to develop specific metrics for transitioning custom and semi-custom advanced microelectronics (e.g., GPUs, FPGA, and ASICs) to programs of record. These metrics should capture the transition plans and milestones for existing microelectronics research programs across the DoD R&E enterprise, including the Defense Advanced Research Projects Agency's (DARPA) Electronics Resurgence Initiative and the Trusted & Assured Microelectronics program. It should also feature narrative descriptions of the impact to mission of successful transitions. Transition metrics should also identify milestones for scaling the manufacturing of SOTA, AI-enabling electronic components developed through research efforts to meet the needs of DoD programs. For commercialization, metrics should track the success of intellectual property sharing with the commercial sector for microelectronics programs.

[87] Department of Defense, Office of the Secretary of Defense, *Department of Defense Fiscal Year 2021 Budget Estimates: Research Development, Test & Evaluation, Defense-Wide*, Vol. 3 of 5 (Feb. 2020), https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2021/budget_justification/pdfs/03_RDT_and_E/RDTE_Vol3_OSD_RDTE_PB21_Justification_Book.pdf.

# ISSUE #2: ENSURE NEAR, MEDIUM, AND LONG-TERM LEADERSHIP IN ADVANCED MICROELECTRONICS ARCHITECTURES

The slow down of Moore's Law scaling means that the relative gains from each generation of computing are decreasing. Future generations of chips could also face diminishing marginal returns, especially as lithography techniques reach anatomical limits. Should this trend continue, the relative advantage the United States has enjoyed in cutting-edge hardware will decrease over time, even if foreign competitors remain two generations behind industry leaders in semiconductor design, as is currently the case.[88] In order to ensure continued U.S. dominance in microelectronics in the near-to-medium-term, it will be necessary to find ways to obtain performance increases in semiconductors by means other than increasing the density of the number of transistors on a chip.

The three primary research arms of the USG focused on microelectronics are DARPA, the National Science Foundation (NSF), and the Department of Energy (DOE). The following recommendations focus on bolstering the activities of each of these agencies, while also facilitating contributions from agencies that do not currently engage in microelectronics R&D but have the capability to do so.

## *Recommendation 2: Maintain global leadership in microelectronics by clearly stating research priorities, increasing USG R&D funding, and articulating a national strategy for microelectronics and associated infrastructure (e.g., a national microelectronics laboratory and incubator).*

*Proposed Executive Branch Actions*

### *Recommendation 2-1: Prioritize research into beyond-CMOS AI hardware capabilities for national security applications.*

The USG must prioritize R&D into technologies and techniques that can extend the life of classical computing, ensuring continued growth in processing power until potential alternative computing architectures such as quantum or neuromorphic computing are readily available. Doing so will be key to ensuring that the United States continues to out-innovate its competitors, particularly as China continues to invest heavily in its domestic semiconductor industry (see Appendix for background).

Due to the high costs associated with scaling power and frequency in microelectronics, industry is pursuing performance gains—particularly for Ai—through chip specialization. The result has been specialized GPUs, TPUs, ASICs, or FPGAs which are more efficient at processing AI algorithms than traditional CPUs. While these chips have achieved notable performance gains,

[88] Josh Horwitz and Sijia Jiang, *China Chip Industry Insiders Voice Caution on Catch-up Efforts*, Reuters (June 13, 2019), https://www.reuters.com/article/us-huawei-tech-usa-chip-catchup-analysis/china-chip-industry-insiders-voice-caution-on-catch-up-efforts-idUSKCN1TE1R4.

they will likely not be a primary driver of long-term performance growth. Specialization faces diminishing marginal returns over time; if advancement of the underlying microprocessors slows, future gains from increased specialization alone will be insufficient to spur significant performance increases. This may lead to market failures, as firms may not see it in their short-term interest to invest in the R&D necessary to lay the foundation for long-term advancements in microelectronics.[89] As a result, government investment is required to spur long-term research and development.

To complement ongoing efforts, the Commission wishes to highlight for Executive Branch agencies and Congress specific, beyond-CMOS hardware capabilities that the Commission believes will be essential to ensure the United States maintains its current edge in advanced AI-related hardware. In particular, the Commission believes that DARPA and the NSF should prioritize programs which focus on research involving 3D chip stacking, photonics, carbon nanotubes, Gallium Nitride (GaN) transistors, domain specific hardware architecture, and electronic design automation, and cryogenic computing. These represent technologies which the Commission assesses are key to ensuring the continued growth of compute and mitigate the impacts of the slowdown of Moore's Law. While there has been limited USG-funded research on these topics, USG funding has been heavily weighted towards applied research, rather than the basic research that is necessary to achieve breakthroughs.

*Proposed Funding Actions*

## *Recommendation 2-2: Increase the budget of DARPA's Electronics Resurgence Initiative to $500 million.*

The Electronics Resurgence Initiative (ERI) is DARPA's primary mechanism for funding advanced microelectronics research, investing approximately $250-300 million annually. Much of this program specifically targets beyond-CMOS architectures, funding both applied sciences and basic research at approximately a 5:1 ratio. Since FY 2019, DARPA's funding request for ERI-related programs has declined. Meanwhile, the Administration's FY 2021 overall budget request for DARPA included a 13 percent increase over FY 2019 levels.[90] Given the need to achieve microelectronics breakthroughs to ensure continued and long-term leadership in AI, particularly in the area of advanced fabrics and post-CMOS architectures, these two funding streams must move in tandem with one another, not in opposite directions.

DARPA's work on advanced microelectronics is both underfunded relative to the magnitude of the problem set, and currently trending in the wrong direction. In 2018, the Defense Science Board (DSB) recommended that DARPA increase funding for ERI to $450 million to accelerate the discovery of advanced microelectronics fabrics.[91] This option would endorse and build on

[89] GlobalFoundries' decision not to operate a 7 nanometer node and to decrease funding for cutting-edge R&D, and instead invest in specialization and packaging techniques, highlights these trends within industry. For more information see: Anton Shilov & Ian Cutress, *GlobalFoundries Stops All 7nm Development: Opts to Focus on Specialized Processes*, AnandTech (Aug. 27, 2018), https://www.anandtech.com/show/13277/globalfoundries-stops-all-7nm-development/2.

[90] Department of Defense, Office of the Secretary of Defense, *Department of Defense Fiscal Year 2021 Budget Estimates: Research Development, Test & Evaluation, Defense-Wide*, Vol. 1 of 5 (Feb. 2020), https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2021/budget_justification/pdfs/03_RDT_and_E/RDTE_Vol1_DARPA_MasterJustificationBook_PB_2021.pdf.

[91] Defense Science Board, *Quick Task Force on Technology Strategy* (2018).

the DSB recommendation, recommending that the budget for ERI increase to $500 million in FY 2021.

## *Recommendation 2-3: Increase NSF's topline budget by $50 million directed toward microelectronics and semiconductors research for enhancing AI capabilities.*[92]

The National Science Foundation's budget for semiconductors and microelectronics research has declined approximately 10 percent since FY 2019, from $92.59 million to $84.16 million in the FY 2021 budget request.[93] Meanwhile, NSF's FY 2021 request for AI represents an 81 percent increase over the FY 2019 allocated funding. While the NSF's AI-related funding increase has been highlighted, the decrease in semiconductors and microelectronics R&D is a misstep given the critical relationship between leadership in AI-related hardware R&D and leadership in AI writ large. AI applications are inherently reliant on semiconductors and microelectronics for their functionality, and research into both advanced microelectronics fabrics and technologies relevant to specialized AI-related chipsets will enable significant future performance gains and AI capabilities. Congress should appropriate an additional $50 million to the NSF FY 2021 budget and highlight the importance of research into semiconductors and microelectronics targeted to enhance AI capabilities.[94] This increased funding level would reverse the decline in funding for basic research in advanced microelectronics design techniques.

## *Recommendation 2-4: Fund a pilot $20 million prize challenge for AI-enabled hardware through IARPA.*

Intelligence Advanced Research Projects Activity (IARPA) currently has no programs focused on advanced chip design after concluding the Trusted Integrated Circuits (TIC)[95] and Rapid Analysis of Various Emerging Nanoelectronics (RAVEN)[96] programs, both of which focused on microelectronics. This is a notable gap, given IARPA's history of successful programs in this area. IARPA could leverage its successful history of running "prize challenges" to invite industry and academia to attempt breakthrough high-risk, high-payoff research. Drawing on this track record, IARPA could establish a new prize challenge focused on advanced chip design and AI-enabling microelectronics. This challenge, or series of challenges, could attempt to spur innovation towards specific goals, such as developing secure electronic design automation (EDA) libraries, or shrinking the time to transition from an algorithm to an ASIC in one year. Congress should appropriate $20 million to IARPA in FY 2021 to run a pilot program creating prize challenges specifically associated with advancing AI-enabled hardware, with the goal of spurring advances in scaling post-Moore's law. Should this prove successful and scalable, IARPA can evaluate whether expanding the program by adding additional resources in future years would prove beneficial.

[92] See Tab 1, recommendation 1. This recommendation describes in detail the justification for the proposed $50 million in additional funding to NSF to support research into semiconductors and microelectronics necessary for AI-related hardware, as first described in Tab 1—which describes the recommendation for $450 million in total NSF budget increases.

[93] National Science Foundation, *FY 2021 Budget Request to Congress* (Feb. 10, 2020), https://www.nsf.gov/about/budget/fy2021/pdf/fy2021budget.pdf.

[94] Congress does not specify how NSF should distribute funding across these directorates and their component divisions. It does, however, provide policy guidance on selected matters.

[95] Intelligence Advanced Research Projects Activity, *Trusted Integrated Chips*, https://www.iarpa.gov/index.php/research-programs/tic.

[96] Intelligence Advanced Research Projects Activity, *Rapid Analysis of Various Emerging Nanoelectronics*, https://www.iarpa.gov/index.php/research-programs/raven.

*Proposed Legislative Branch Action*

### *Recommendation 2-5: Require the USG to develop a national microelectronics strategy within 180 days and assess the viability of a national microelectronics laboratory and incubator.*

The United States lacks a national strategy for microelectronics to support interagency coordination within the USG externally with industry and academia. A truly national strategy would build on DoD's Microelectronics Innovation for National Security and Economic Competitiveness program and previous studies conducted by the U.S. Government or on its behalf. Expanding beyond DoD, it would leverage the expertise and perspectives of the interagency to produce a fully coordinated approach to microelectronics.[97] Given the urgent and cross-cutting nature of the problem, it is critical that DoD's approach be integrated with actions taken by Commerce and State, as well as other relevant agencies, to promote domestic R&D of microelectronics and prevent the illicit transfer of technology to competitors. The United States also faces infrastructure and funding gaps for microelectronics research, development, and commercialization in the public and private sectors, all of which are important for maintaining U.S. leadership in semiconductors. The United States must continue innovating at the cutting edge of semiconductors to strengthen the U.S. economy and mitigate the threat posed by Chinese industrial policy and corresponding investments.[98] A U.S. strategy would foster a coordinated approach and help overcome looming challenges to microelectronics innovation, competitiveness, and supply chain integrity. DoD, in coordination with other relevant departments and agencies including the DOE, ODNI, the Department of State, the Department of Commerce, and NSF, could develop the strategy within six months of the passage of the NDAA, drawing on the findings of the 2017 President's Council of Advisors on Science and Technology report on semiconductor leadership,[99] the 2019 DSB's Summer Study, and DoD's existing strategy for assured access to trusted microelectronics.[100] This strategy would build on previous studies and strategies by focusing on AI-enabling performance, research funding priorities, interagency and international coordination, and private sector partnerships.

The Commission recommends the FY 2021 NDAA include language requiring the creation of a national strategy with components focused on national security, U.S. leadership, and competitiveness, within 180 days. The Commission also recommends establishing a senior leadership panel composed of the National Security Council, the National Economic Council, the Office of Science and Technology Policy, and relevant departments and agencies within 30 days

[97] Interagency Task Force in Fulfillment of Executive Order 13806, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States* (Sept. 2018), https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF; Daniel J. Radack et. al., *Semiconductor Industrial Base Focus Study – Final Report*, Institute for Defense Analyses (Dec. 2016), https://www.ida.org/-/media/feature/publications/s/se/semiconductor-industrial-base-focus-study--final-report/d-8294.ashx; National Academies of Sciences, Engineering, and Medicine, AS USAF, *The Growing Threat to Air Force Mission-Critical Electronics* (2019), https://www.nap.edu/catalog/25475/the-growing-threat-to-air-force-mission-critical-electronics-lethality.

[98] The President's Council of Advisors on Science and Technology (PCAST), *Report to the President: Ensuring Long-Term U.S. Leadership in Semiconductors* (Jan. 2017), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_ensuring_long-term_us_leadership_in_semiconductors.pdf.

[99] *Id.*

[100] The National Defense Authorization Act for Fiscal Year 2017 included a reporting requirement (Sec. 233) mandating that DoD develop a strategy for assured access to trusted microelectronics. Pub. L. 114-328.

to oversee U.S. microelectronics leadership and competitiveness. The legislative language should also require that the Secretary of Defense and Assistant to the President for National Security Affairs provide an interim briefing to Congress after 90 days regarding the strategy's status, and report any initial findings and conclusions.

As part of this strategy, the Secretary of Defense—in coordination with the Secretary of Energy and Director of National Intelligence—should consider the viability, efficacy, and cost of developing a national laboratory exclusively focused on microelectronics research and development. Such a laboratory could serve as a hub for federal research into breakthrough microelectronics-related technologies,[101] as well as an incubator for early-stage semiconductor startups which currently face difficulties scaling due to the high costs of microelectronics design and fabrication.[102] The incubator could provide resources to promising, early-stage microelectronics startups, while also giving them access to fabrication facilities, design tools, and shared intellectual property to assist with early-stage development costs. This laboratory could also become a center for government expertise in high-performing, trusted microelectronics, ensuring continued U.S. leadership in this field over the ensuing years.

The national strategy should also consider the role of diplomacy and trade in maintaining U.S. microelectronics leadership. In particular, it should assess the potential impact of approaches to multilateral export controls tailored for specific semiconductor manufacturing equipment (e.g., extreme ultraviolet photolithography equipment and argon fluoride immersion photolithography equipment) through direct coordination with key U.S. allies, the Wassenaar Arrangement, and other multilateral fora.[103] It should also analyze if additional U.S. trade enforcement actions are necessary in light of China's extensive semiconductor subsidy program. Finally, it should assess options for increasing the competitiveness of the U.S. semiconductor industry through the elimination of policies that harm U.S. companies without producing a substantial benefit to U.S. national security (e.g., trade barriers and uniliteral export controls).

## ISSUE #3: THE UNITED STATES LACKS A CREDIBLE ALTERNATIVE TO HUAWEI AND IS FALLING BEHIND IN THE GLOBAL RACE FOR 5G DEVELOPMENT AND IMPLEMENTATION, WHICH WILL DIRECTLY IMPACT THE NATION'S ABILITY TO UTILIZE AI AT SCALE.

[101] This would build off of and expand upon the model set by DOE's Science and Innovation hubs (https://www.energy.gov/science-innovation/innovation/hubs), which serve as basic and applied research centers for specific topics. Given the scope and expense of the microelectronics field, this model would be scaled up to be on par with the funding of larger FFRDCs.

[102] Semiconductor startups face challenges getting access to advanced fabrication facilities due to their expense, relative rarity, and long wait times. This presents a market failure that the government is well suited to fill, granting limited run-times to startups producing products which show promise for national security applications.

[103] As of 2015, the United States, Japan, and the Netherlands contained over 90% of the global SME industry, including the eight largest SME firms. Photolithography tools, the most complex and expensive type of SME, are even more concentrated, with one active Dutch company (ASML) and two active Japanese companies (Nikon and Canon). For additional information, see David Manners, *Top Ten Foundries 2017*, Electronics Weekly (Dec. 1, 2017), https://www.electronicsweekly.com/news/business/top-ten-foundries-2017-2017-12/; and Peter Clarke, *ASML Increases Dominance of Lithography Market*, eeNews Analog (Feb. 12, 2018), https://www.eenewsanalog.com/news/asml-increases-dominance-lithography-market.

The Commission's mandate requires it to address "artificial intelligence, machine learning, and associated technologies." The Commission's interim report identified three key associated technologies for which it will provide recommendations: 5G, quantum computing, and biotechnology. However, given the urgent need to address 5G, it is providing select, immediate options Congress can implement now to help expand the domestic 5G network and create a global alternative to Huawei.

5G networks will form the connective tissue between AI platforms. Ensuring the United States maintains access to trusted and robust 5G networks is a critical component of overall leadership in AI. This is particularly true as microelectronics continue to advance, and the capability to run sophisticated AI models at the edge will increase. As AI becomes more dispersed throughout the network, the need for a secure and effective 5G network will increase even more.

Huawei is pursuing global dominance in 5G and the United States has been unable to convince even its closest allies and partners to completely exclude Huawei hardware and software from their 5G networks. Faced with this reality, immediate action is necessary to create a Western supplier that can compete with Huawei both in price and quality. Due to the urgency of the issue, the United States should pursue several complementary approaches concurrently to maximize the chance of success.

## *Recommendation 3: Pursue policies and funding opportunities which advance spectrum-sharing and 5G commercial licensing, as well as R&D into 5G software, hardware, microprocessing technology, and open-access radio networks, as part of a portfolio approach to accelerating 5G adoption in the United States and fostering global alternatives to Huawei.*

*Proposed Funding Actions*

### *Recommendation 3-1: R&D efforts should be appropriately resourced to develop and improve 5G spectrum sharing, particularly in the sub-6 GHz mid-band spectrum.*

AI systems require high fidelity sensing as well as fast, safe, and secure networks. It is a national security imperative for the U.S. military to have access to a powerful 5G network to enable future AI capabilities, and ensure the network is trusted to prevent competitors from accessing our AI systems. The United States must preserve this access and trust while building its 5G network. The sub-6 GHz spectrum, sometimes referred to as mid-band or the goldilocks band of spectrum, is a critical portion of the spectrum for both DoD and commercial 5G operations. It is currently used by many radar and communication systems within the DoD, as radars and sensors operating in the sub-6 GHz region of spectrum combine high discrimination capability with long range operations. Sub-6 GHz is also critical for 5G civilian communications since it provides high data rates together with good range and penetration.

Given that sub-6 GHz is important for both sensing using radar and communications, spectrum sharing research is particularly important to enable access for both purposes simultaneously.

However, current spectrum sharing capabilities are not optimized.[104] Additional technical development on spectrum sharing, particularly in utilizing AI to dynamically manage spectrum access, is still necessary to fully utilize the available spectrum for sharing. Implementation of improved spectrum sharing technologies could make more mid-band spectrum available for civilian and commercial use while preserving critical DoD systems for sensing. The Commission supports increased research and development to improve the U.S. government's ability to share the sub-6 GHz mid-band spectrum with 5G operators for commercial and civilian use.

*Proposed Executive Branch Actions*

### *Recommendation 3-2: Urge the FCC, DoD, and NTIA to work to expand sub-6 GHz spectrum-sharing arrangements and licenses for commercial 5G use, which minimizes risk to DoD operations while expanding the availability of commercial 5G bandwidth.*

The slow rollout of 5G networks in the United States, which currently has one-fifteenth of the number of deployed 5G-operable base stations compared to China,[105] risks slowing U.S advances in AI, both in the government and the private sector.[106] The lack of U.S. mid-band spectrum commercial availability, combined with the high capital requirements necessary to ensure coverage utilizing high-band spectrum, have substantially slowed the deployment of 5G networks. Furthermore, the high-band is losing out to mid-band as the global standard, as other countries face less spectrum-crowding in the mid-band and are more willing to adopt it as their standard. This trend is exacerbated by Huawei's emphasis on the mid-band, and the $75 billion that the Chinese government has given it in subsidies.[107]

The USG is working to address this problem by developing spectrum sharing capabilities within the 3 to 6-GHz range. In 2015, the FCC established the Citizens Broadband Radio Service (CBRS), the first U.S. spectrum sharing model. Since that time, the NTIA has studied, and has collaborated with the DoD and FCC, on maximizing spectrum sharing capabilities.[108] The CBRS enables shared federal and non-federal use of the band. This work will enable the U.S. Navy and non-government providers to share the 3550-3700 MHz band, and will be divided into three, dynamically-managed tiers: the Navy will maintain first priority access, followed by companies and organizations which purchase priority-access licenses, and finally companies and

[104] For information about existing spectrum sharing test beds, see Defense Advanced Research Projects Agency, *World's Most Powerful RF Emulator to Become National Wireless Research Asset* (Sept. 3, 2019), https://www.darpa.mil/news-events/2019-09-03. For details on current spectrum sharing programs, see Recommendation 3-2 below.

[105] Stu Woo, *In the Race to Dominate 5G, China Springs Ahead*, Wall Street Journal (Sept. 7, 2019), https://www.wsj.com/articles/in-the-race-to-dominate-5g-china-has-an-edge-11567828888.

[106] The U.S. Department of Defense is allocated by the National Telecommunications and Information Administration (NTIA) a significant percentage of the mid-band, defined as spectrum in the 3 to 6-GHz range, and the FCC has not yet licensed any mid-band spectrum for commercial 5G use. Instead, it has held auctions in the high-band spectrum range, defined as spectrum between 24 and 300-GHz.

[107] Chuin-Wei Yap, *State Support Helped Fuel Huawei's Global Rise*, Wall Street Journal (Dec. 25, 2019), https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

[108] Edward Drocella, Robert Sole, & Nickolas LaSorte, *Technical Feasibility of Sharing Federal Spectrum with Future Commercial Operations in the 3450-3550 MHz Band*, NTIA (Jan. 27, 2020), https://www.ntia.gov/report/2020/technical-feasibility-sharing-federal-spectrum-future-commercial-operations-3450-3550.

organizations that register at no cost.[109] The FCC will hold an auction for priority-access licenses for this band in July 2020.[110] Expanding such sharing efforts is critical, as it will ensure that DoD maintains access to spectrum which is essential for operational effectiveness, while also broadening commercial access to spectrum which can be utilized for 5G networks. In April 2019, the Defense Innovation Board issued a report which argued that the status quo of spectrum allocation is unsustainable and DoD must expand its sub-6GHz spectrum sharing operations to enable the United States to compete with China in 5G.[111]

The Commission urges the FCC, DoD, and NTIA to expand spectrum-sharing programs such as the CBRS, and work to license additional sub-6GHz spectrum to wireless carriers and equipment makers for commercial 5G use. Sharing and licensing additional mid-band spectrum will ensure unrestricted DoD access in the event of an emergency. By expanding commercial access to the mid-band, it will also allow the United States to more quickly develop its domestic 5G networks and develop ways and means to compete with Huawei globally.

*Proposed Legislative Branch Action*

### *Recommendation 3-3: Pass the Utilizing Strategic Allied (USA) Telecommunications Act.*

The bipartisan USA Telecommunications Act, introduced by Senators Warner, Burr, Rubio, Menendez, Cornyn, and Bennett, provides $750 million in funding for R&D of 5G software, hardware, and microprocessing technology, including open-access radio networks (O-RAN). O-RAN would allow multiple firms to use the same radio access network rather than relying on proprietary hardware. Given that 60 to 65 percent of the cost of ownership of a network is in developing the radio access network,[112] creating an O-RAN network would substantially lower the costs of developing a 5G network for U.S. and allied firms. Combined, these R&D efforts would also directly counter Huawei's biggest advantage, which is inexpensive, proprietary hardware. Furthermore, by standardizing 5G hardware it would shift the differentiating factor in 5G to software, which plays to existing U.S. strengths due to the substantial technical advantages possessed by U.S. firms. All major U.S. telecoms and most major European telecom companies are actively supporting the development of O-RAN efforts.[113] Huawei is the most significant provider in the world opposing O-RAN development. The USA Telecommunications Act would be a first step toward posturing U.S. and allied firms to better compete with Huawei on 5G.

[109] Commscope, *Spectrum Access System Frequently Asked Question*, https://www.commscope.com/solutions/5g-mobile/spectrum-management-solutions/spectrum-access-system-faqs/.
[110] Federal Communications Commission, *FCC Changes Upcoming Auction 105 Schedule, Postpones Auction 106* (Mar. 25, 2020), https://docs.fcc.gov/public/attachments/DOC-363292A1.pdf.
[111] Defense Innovation Board, *The 5G Ecosystem: Risks & Opportunities for DoD* (Apr. 2019), https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF.
[112] Samsung, *The Open Road to 5G*, https://image-us.samsung.com/SamsungUS/samsungbusiness/pdfs/Open-RAN-The-Open-Road-to-5G.pdf.
[113] O-RAN Alliance, *Membership*, https://www.o-ran.org/membership.

# APPENDIX: BACKGROUND AND CONTEXT ON MICROELECTRONICS AND AI

## I. *Global Trends in Microelectronics*

AI applications are inherently reliant on hardware to enable their functionality, and currently this hardware is almost exclusively fueled by integrated circuits. As a result, the demand for semiconductors to enable AI applications is expected to grow dramatically within the coming years. McKinsey & Company estimates that the total demand for non-AI-related semiconductors is expected to grow by 32% from 2017 to 2025 (from $223 billion to $295 billion) and the demand for AI-related semiconductors is expected to grow by 282% over that same timeframe (from $17 billion to $65 billion).[114] As AI becomes more widespread and advanced, the demand for sophisticated and specialized chipsets to run those algorithms will likely increase. This AI-driven demand for computer chips is already changing the nature of semiconductor R&D, with less focus on general-purpose computer chips like central processing units (CPUs) and more focus on specialized computer chips that can exhibit higher speed, improved energy efficiency, and smaller mobile form factors for AI systems. While 97% of training algorithms were run on off-the-shelf graphics-processing units (GPUs) as of 2017, McKinsey estimates that by 2025 this market share will shrink to 40%, while 50% of the market will be run on application-specific integrated circuits (ASICs) and 10% on Field Programmable Gate Arrays (FPGAs), with the latter category likely capturing predominantly the bespoke rather than commercial market.[115]

This transition from GPUs to ASICs and FPGAs will mean the demand for chipsets tailored to specific processes will increase, placing a premium on chipset design and fabrication capabilities and experience. The semiconductor industry manufactures computer chips specialized for training and execution (also called "inference") of machine learning systems. Furthermore, as employment of AI systems on the edge increases, especially execution ("inference") of AI systems, the ability to produce advanced semiconductors for use on consumer electronics devices at scale becomes even more important. Complex semiconductor supply chains are necessary to fabricate advanced semiconductors like GPUs, ASICs, and FPGAs. Facilities called fabs (also called "foundries") use semiconductor manufacturing equipment (SME) to manufacture semiconductors based on chip designs.

Any country, or group of countries, which has an advantage in access to high-end chipsets will have an inherent advantage in their ability to deploy high-performing AI algorithms. The market for high-end chipsets is global, with firms currently able to purchase cutting-edge off the shelf chipsets largely regardless of location.

### *United States*

Although U.S. firms account for nearly half of all semiconductor production, not all of these chips are produced in the United States. Increasingly, U.S. firms are moving away from the traditional vertically integrated device manufacturer (IDM) model, in which firms design and manufacture the chips. Instead, firms are moving toward a "fabless" model in which the design of the chip occurs in-house, but its fabrication is outsourced to a third-party foundry, and assembly, testing, and packaging (ATP) is outsourced to a dedicated ATP firm. NVIDIA, Qualcomm, and

[114] Gaurav Batra, et al, *New Opportunities for Semiconductor Companies*, McKinsey & Company (Dec. 2018), Exhibit 3, https://www.mckinsey.com/industries/semiconductors/our-insights/artificial-intelligence-hardware-new-opportunities-for-semiconductor-companies.

[115] *Id.* at Exhibit 6.

Broadcom are among the major U.S. players that have adopted the fabless model, while industry-leaders Intel and Korean-owned Samsung maintain the IDM model. Approximately 49% of U.S. semiconductors are fabricated in the United States, while 51% are produced outside the country.[116] Among third party foundries, Taiwan Semiconductor Manufacturing Company (TSMC) maintains an enormous market share, capturing 55.9% of the foundry market in 2017. The top four foundries – TSMC (Taiwan), Global Foundries (United States), United Microelectronics Corporation (Taiwan), and Samsung (Korea) – accounted for 81.5% of the overall foundry market share.[117] In terms of chip design, U.S.-based NVIDIA has led the GPU industry for several years but there are indications that China is catching up. In September 2019, Chinese company Alibaba released its Hanguang-800 chips, which beat Intel and NVIDIA on standard deep-learning benchmarks.[118]

While the U.S. semiconductor industry was once heavily government-financed, it is now largely financially independent from the USG. In the early 1980s, DoD accounted for 90% of all U.S. semiconductor purchases (at that time U.S. companies had a 60% share of the global market and Japanese companies had a 35% share). As of 2017, DoD purchases accounted for approximately 0.5% of global semiconductors, a precipitous decline.[119] While this change largely reflects the global growth in the commercial semiconductor industry, it has also had a profound impact on the ability of the USG to induce firms to work toward U.S. national objectives and retain access to assured microelectronics, particularly if it could mean compromising access to lucrative foreign markets.

### *China*

China is the largest market for semiconductors in the world, but Chinese technology firms are also heavily reliant on U.S. semiconductors to sustain their operations. China recognizes its vulnerability in the integrated circuits sector and has taken steps to increase its self-sufficiency and domestic market share. In 2014, the Chinese Government released its "Guidelines to Promote National Integrated Circuit Industry." The Ministry of Industry and Information Technology (MIIT) and the Ministry of Finance subsequently established the National Integrated Circuit Investment Fund. This government-run fund is tasked with acquiring companies along the semiconductor value chain in order to decrease China's reliance on semiconductor imports. It raised 138.7 billion yuan (about $22 billion) in its first round in 2014.[120] By the end of 2017, it had invested 81.8 billion yuan (about $12.6 billion) into 67 projects, with a total investment commitment of 111.8 billion yuan.[121] Reports from July 2019 indicate a second round has raised 200 billion yuan (about $29 billion).[122] However, U.S. firms have control over 95% of the Chinese

[116] NSCAI interview with Semiconductor Industry Association.

[117] David Manners, *Top Ten Foundries 2017*, Electronics Weekly (Dec. 1, 2017), https://www.electronicsweekly.com/news/business/top-ten-foundries-2017-2017-12/.

[118] Catherine Shu, *Alibaba Unveils Hanguang 800, an AI Inference Chip it Says Significantly Increases the Speed of Machine Learning Tasks*, TechCrunch (Sept. 25, 2019) https://techcrunch.com/2019/09/24/alibaba-unveils-hanguang-800-an-ai-inference-chip-it-says-significantly-increases-the-speed-of-machine-learning-tasks/

[119] Advisory Panel on Streamlining and Codifying Acquisition Regulations, *Section 809 Panel Interim Report* at 19 (May 2017), https://section809panel.org/wp-content/uploads/2017/05/Sec809Panel_Interim-Report_May2017_FINAL-for-web.pdf.

[120] Sarah Dai, *China Completes Second Round of US$29 Billion Big Fund Aimed at Investing in Domestic Chip Industry*, South China Morning Post, (July 2019), https://www.scmp.com/tech/science-research/article/3020172/china-said-complete-second-round-us29-billion-fund-will

[121] Elaine Chan, *Made in China 2025: How New Technologies could Help Beijing Achieve its Dream of Becoming a Semiconductor Giant*, South China Morning Post (Sept. 24, 2018), https://www.scmp.com/business/article/2165575/made-china-2025-how-new-technologies-could-help-beijing-achieve-its-dream.

[122] Yoko Kubota, *China Sets up New $29 Billion Semiconductor Fund*, Wall Street Journal (Oct. 25, 2019), https://www.wsj.com/articles/china-sets-up-new-29-billion-semiconductor-fund-11572034480.

market share in the markets for critical AI-related sub-product categories (GPUs, CPUs, and FPGAs) in China, U.S. firms have over a 95% market share, despite significant Chinese investment in national champion semiconductor firms.[123] To date, the focus of China's semiconductor industry has been memory, recognizing that the aforementioned categories are dominated by U.S. firms. China is heavily dependent on imported semiconductor manufacturing equipment (SME), and has no capacity to produce the most advanced equipment, all of which is either made in the United States, Japan, or the Netherlands.[124]

Additionally, the Made in China 2025 Initiative specifically names integrated circuits as an area that requires domestic investment. The Made in China "roadmap" related to integrated circuits calls for 16 and 14 nanometer production levels (approximately one or two generations behind current industry-leaders) to achieve scale production at the "advanced international level" by 2020 with a full domestic supply chain, and for China to compete with all industry leaders by 2030.[125] China is likely anticipating that as Moore's Law comes to an end, industry's ability to iterate will slow and it may have an opportunity to catch up to global leaders more quickly.

## *II. Hardware Opportunities for National Security and AI Advantage*

As described in the previous section, shifting electronics supply chains have reduced U.S. domestic advanced technology manufacturing and packaging capacity. DoD's existing access to trusted commercial hardware through the Defense Microelectronics Activity (DMEA) trails several generations behind SOTA. Despite these trends, the Commission is encouraged by ongoing USG efforts to address systemic challenges, including DARPA's Electronics Resurgence Initiative (ERI) and the Trusted & Assured Microelectronics program.

The USG has unique constraints and requirements for microelectronics compared to the commercial sector, including high security and reliability in unique environments (e.g., radiation hardening); small production volumes; and long lifecycle timelines (e.g., maintaining legacy systems). These requirements and constraints also apply to specialized AI chips. Deputy Under Secretary of Defense for Research and Engineering Dr. Lisa Porter highlighted these requirements in October 2019, specifically noting that machine-learning inference engines at the edge will demand leading-edge technology to meet very stringent performance and power requirements.[126]

But, in addition to unique constraints, AI chips can also confer unique advantages for national security applications in terms of performance and efficiency. FPGAs, ASICs, and GPUs can offer specific and unique AI-enabled capabilities compared to CPUs in a variety of mission areas including electronic warfare; Intelligence, Surveillance, and Reconnaissance (ISR) (specifically target recognition, radar, undersea acoustics, and space systems); secure communications; and autonomous or semi-autonomous systems operating at the edge. Specific advantages of AI specialized chips for edge applications include 1) lower communication bandwidth requirements for operation in contested environments 2) faster response times 3) higher performance in terms of accuracy and precision 4) greater power efficiency and 5) improved data security because sensory data is maintained on the local device.

[123] NSCAI interview (Sept. 17, 2019).

[124] Peter Clarke, *ASML Increases Dominance of Lithography Market*, eeNews Analog (Feb. 12, 2018), https://www.eenewsanalog.com/news/asml-increases-dominance-lithography-market.

[125] U.S. Chamber of Commerce, *Made in China 2025: Global Ambitions Built on Local Protections* at 65 (2017), https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf.

[126] Dr. Lisa Porter, *The U.S. Defense Department's New Thinking on Microelectronics Security*, Department of Defense (2019), 612ydhttps://science.dodlive.mil/2019/09/10/the-defense-departments-new-thinking-on-microelectronics-security/.

# LIST OF KEY ACRONYMS[127]

ACD&P - Advanced Component Development and Prototypes

ASIC - Application Specific Integrated Circuit

ATP - Assembly, Testing, and Packaging

BEOL - Back-End-of-Line

CBRS - Citizens Broadband Radio Service

CMOS - Complementary Metal Oxide Semiconductor

COTS - Commercial-Off-the-Shelf

DARPA - Defense Advanced Research Projects Agency

DMEA - Defense Microelectronics Activity

DoD - Department of Defense

DOE - Department of Energy

EDA - Electronic Design Automation

ERI - Electronics Resurgence Initiative

GaN Transistor - Gallium Nitride Transistor

GOTS - Government-Off-the-Shelf

GPU - Graphics Processing Unit

FEOL - Front-End-of-Line

FPGA - Field Programmable Gate Array

IDM - Integrated Device Manufacturer

IP - Intellectual Property

MCP - Multi-Chip Packages

NSF - National Science Foundation

NSWC Crane - Naval Surface Warfare Center Crane

[127] For definitions of many of these terms, see NIST's Computer Security Resource Center, at https://csrc.nist.gov/glossary/.

NTIA - National Telecommunications Information Administration

O-RAN - Open-Access Radio Networks

OTA Agreement - Other Transaction Authority Agreement

OUSD(R&E) - Office of the Under Secretary of Defense for Research and Engineering

RAVEN Program - Rapid Analysis of Various Emerging Nanoelectronics Program

RDT&E - Research, Development, Test, and Evaluation

SOTA - State of the Art

SHIP - State-of-the-Art Heterogeneously Integrated Packaging

SDD - System Development and Demonstration

SME - Semiconductor Manufacturing Equipment

SWaP - Size, Weight, and Power

TIC Program - Trusted Integrated Circuits Program

# 5. Recommendations to Improve AI Cooperation Among Key Allies and Partners

TAB 5

The Commission's Interim Report highlighted the national security imperative to develop AI alliances and partnerships. The United States' security and technology relationships are a sound basis on which to build an AI cooperation framework. The fundamentals of such a framework include cooperative planning, data sharing, research, development, procurement, standards, and interoperability. AI cooperation along these lines can help us achieve the goals in our National Security and Defense Strategies.

The Commission's Interim Report noted that "the Five Eyes Alliance is a good place to start because the United States can leverage existing technical cooperation and information-sharing agreements."[128] The Five Eyes are an established intelligence network of allied countries that actively share information and cooperate on defense and security across a range of areas. With respect to AI, the Five Eyes nations have leading talent and significant commercial and research capacities. When well-coordinated, these capacities are robust and effective. The Commission has developed a series of early recommendations with Five Eyes partners at the center.

We have found, however, that an exclusive focus on the Five Eyes would be insufficient to address our strategic challenges. The United States needs to cultivate AI cooperation among the broad and deep network of allies and partners that it enjoys—and especially among those who are willing and able to contribute significant security-related technology capabilities.

Our initial recommendations begin to address dimensions of Five Eyes and broader allied cooperative planning, data sharing, procurement, and interoperability. The Commission will continue to develop options for cooperation with other key U.S. allies and partners in subsequent recommendations.

## ISSUE #1: LACK OF A NATIONAL SECURITY POLICY FRAMEWORK FOR AI COOPERATION

The U.S. government lacks a coherent national security policy framework for security cooperation with our allies and partners in AI. This is true even for established security relationships such as the Five Eyes, despite the fact that there are approximately 200 Five Eyes-related committees and working groups.[129] A national security policy framework is an urgent need. Improved defense and Intelligence Community collaboration and prioritization could enhance the adoption and impact of AI across Five Eyes, and our broader system of allies and partners. A common vision

[128] The Five Eyes intelligence alliance was formed after World War II. Australia, Canada, New Zealand, the United Kingdom, and the United States are parties to the multilateral UKUSA Agreement, a treaty for intelligence cooperation. Defense and security cooperation among the five countries has grown to encompass a wide range of areas, including in emerging technology and defense innovation.

[129] NSCAI interviews with members of the Intelligence Community, Defense Department, and State Department (Feb. 25, 2020).

would more effectively arrange economic, diplomatic, R&D, military and intelligence elements for competition.

AI cooperation among U.S. allies and partners is nascent, though pockets of innovation are emerging. In particular, current organizational, technical, legal, and policy arrangements are inadequate for achieving allied military interoperability. Yet many allies seek closer cooperation with the United States and its maturing AI-related efforts.

There are promising developments. The Joint Artificial Intelligence Center (JAIC) could be a productive venue for allied cooperation, but is insufficient in and of itself to address the larger challenges of allied AI interoperability. Achieving interoperability, to include integrating collection platforms, data, and processing environments, will likely require agreement on a unique data-sharing framework, distinct from commercial agreements.

Another promising effort is The Technical Cooperation Program AI Strategic Challenge, a Five Eyes initiative. This three-year program examines critical issues for the application of AI as a component of military technology. The Challenge includes four topics: trustworthiness; rationalization; effective transition of AI technologies from science and technology to acquisition and users (coalition warfighters, commanders, and decision makers); and the intersection of AI and international law. While this is a positive effort, it is unfunded and depends on voluntary participation.

*Proposed Executive Branch Actions*

*Recommendation 1-1: The United States should establish a National Security Point of Contact for government-wide AI collaboration with allies at the principal level. The United States should encourage allied governments to do the same.*

*Recommendation 1-2: Under the purview of the National Security Point of Contact, the U.S. government should conduct an assessment of the comparative allied strengths in AI-related technologies and applications, beginning with the Five Eyes and then expanding to include NATO and other allies.*

*Recommendation 1-3: Based on the assessment of allied comparative strengths, the U.S. National Security Point of Contact for AI should convene a multilateral working group for AI collaboration and interoperability, beginning with the Five Eyes, to develop a plan for deeper AI collaboration.[130] The plan should include combined research priorities; development objectives; experimentation plans; data sharing agreements; common standards for testing, evaluation, verification, and validation (TEVV) of AI-enabled systems; and*

[130] The 2018 National Defense Strategy cites the requirement to "deepen interoperability" with allies, and DoD's AI Strategy states that the United States should "pioneer AI approaches across the full scale of our global defense enterprise in a manner that is Joint and interoperable with interagency, allied, and coalition partners." DoD recognizes that foreign allies and partners "offer critical perspectives and talent that can be leveraged through personnel exchanges, combined portfolio planning, and the deepened interoperability and trust that comes from collaborative AI development and deployment." See National Defense Strategy, at 9; DoD AI Strategy, at 6, 12.

*interoperability standards and requirements for data, algorithm, communications, and sensor sharing that can be expanded to include our NATO and Asian allies.*[131]

## ISSUE #2: LACK OF AI-RELATED MILITARY CONCEPT AND CAPABILITY DEVELOPMENT WITH ALLIES AND PARTNERS ERODES OUR COMPETITIVE MILITARY ADVANTAGE

Current military concept and capability development efforts among the United States and its allies and partners lack a joint analytical foundation, a common appreciation of threats and opportunities, and ways to stress-test those concepts and capabilities with AI.

U.S. and allied defense communities have not sufficiently articulated innovative and compelling deterrence and warfighting concepts that incorporate AI-enabled capabilities. The Secretary of Defense has directed development of a Joint Warfighting concept for All-Domain Operations, and has identified AI as the Department's number one technology priority.[132] Different thinking is needed by a cadre of allied military, government, and private sector leaders to articulate and operationalize the Secretary of Defense's vision more robustly.

One of the most pressing defense challenges is the need for compatible battle networks.[133] Battle networks are needed across warfighting missions, whether to fight global extremists, regional powers, or a strategic rival. U.S. allies and partners need to enhance and expand interoperable battle networks in order to offset the capabilities of potential adversaries to employ such networks now. Adversaries can employ their networks in ways that threaten to defeat U.S. and allied power projection. Battle networks are now built with commercial technology. Moreover, the networks are more important than the platforms they integrate. Consequently, we must build better networks than our competitors because they have access to the same technology. In 2016, the Defense Science Board concluded that the way to offset these competitor networks is to inject AI and autonomous systems into our battle networks, but we have been slow to do so.[134] Taken together, the U.S. network of allies and partners—including the Five Eyes, NATO, and our Asian allies—possesses significant competitive advantages that can offset those of our adversaries.

[131] Interoperability is a priority for operational concepts, modular force elements, communications, information sharing, and equipment. We understand interoperability to mean the ability to operate across different platforms, systems, domains, services, and partners. It also refers to the ability to digest and utilize data for common protocols and standards. Upgrades and improvements to products can lead interoperability to cease. We believe the future of coalition cooperation lies in "designing out" interoperability problems, by using intelligent technologies that enable more seamless integration across national systems.

[132] "[W]e're in a race, we have to get to the end state quicker than the Chinese can, quicker than the Russians can. And there are a few key technologies out there. I put AI at number one. You know, two, three and four look like directed energy, and hypersonics, and a few other things like that. But at – even with those systems, whether it's hypersonics, directed energy, AI is still going to enable them in – in terms of how you employ them, how you maintain them, all that. So that's why AI to me pops up as number one." Remarks by Secretary of Defense Mark Esper at the NSCAI Strength Through Innovation Conference (Nov. 5, 2019).

[133] In a 2017 interview, former Deputy Secretary of Defense Bob Work articulated this imperative. See William T. Eliason, *An Interview with Robert O. Work*, Joint Forces Quarterly (1st Quarter, 2017), https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1038783/an-interview-with-robert-o-work/.

[134] Defense Science Board, *Summer Study on Autonomy* (June 2016), https://dsb.cto.mil/reports/2010s/DSBSS15.pdf.

Our national security and defense strategies also need to be stress-tested for gaps and opportunities presented by AI and associated technologies. A series of coalition wargames and experiments should be developed, leveraging the wargaming capabilities of the Joint Staff. This series would identify vulnerabilities in our collective and national decision-making processes, concepts, capabilities, and standards. Wargames and experiments would refine our understanding of the most pressing challenges in order to prevent or mitigate strategic vulnerabilities. The Five Eyes would be a strong contributor to such an effort, along with other core treaty allies and trusted partners with strong technology capacities.

Significant opportunities also exist to establish tangible outputs and outcomes to make our warfighting concepts and capabilities more robust. Five Eyes and other allied pilot projects and demonstrations can develop and demonstrate AI-enabled capabilities and concepts, and establish standards based on challenges and opportunities identified through wargaming and experimentation. Joint demonstrations and pilots are ways to begin pursuing a Five Eyes Roadmap for AI and catalyzing innovation needed to compete with our adversaries. Our NATO and other treaty allies should be included, along with partners that have significant academic, commercial, and defense technology capacities.

The United States maintains a strong interest in leading the development of standards to ensure reliable, trustworthy, and responsible AI development with our allies and partners. A multinational effort is needed to develop common standards and methods of testing, verifying, and validating AI systems. Such an effort would further enable the effectiveness and sustainability of the recommendations below.

*Proposed Executive Branch Actions*

*Recommendation 2-1: The Secretary of Defense should designate a point of contact to advance U.S. military concept and capability development cooperation with allies and partners. Concept and capability development would consist of the activities below, with appropriate interagency participation and leadership.*

*Recommendation 2-2: The Secretary of Defense should host an AI Wargame and Experimentation Series, beginning with the Five Eyes, and as appropriate could expand to other allies and partners. AI wargaming and experimentation would inform development of allied and joint warfighting concepts and capabilities for all-domain operations.*

*Recommendation 2-3: The Secretary of Defense and the Director of National Intelligence should conduct several AI demonstration pilot projects with Five Eyes partners over the next three years, some of which should test the use of shared allied cloud computing resources.*

# 6. Recommendations to Advance Ethical and Responsible AI

TAB 6

## ISSUE #1: TRAINING

Building a federal workforce that designs, develops, and fields AI technologies for national security in an ethical and responsible manner requires everyone within the national security enterprise to have a foundational understanding as to what constitutes ethical and responsible AI, including a baseline awareness of the risks and limitations associated with AI systems.

Individuals with specialized roles—like acquisition and procurement professionals, legal personnel, ethics and oversight personnel, and technologists—require more in-depth and tailored training to ensure they are adequately knowledgeable about the responsible and ethical considerations of AI. Only when equipped with such knowledge, will developers and users of AI (and their supervisors) be better prepared to make assessments at each phase of an AI system lifecycle to mitigate potential ethical pitfalls and promote responsible practices. For instance, a procurement official who understands the ethical issues surrounding unwanted bias in AI is more likely to question whether a vendor offering is likely to discriminate based on protected characteristics (either directly or via proxy measures). This type of training is especially critical given that there are no existing standards for fairness and lack of bias in AI systems for procurement officials to rely on. Likewise, a lawyer who understands the need for responsible data governance will be more likely to consider the importance of data use and sharing arrangements, privacy issues specific to AI, and data rights when counseling clients.

### *Recommendation 1: Integrate Ethical and Responsible AI Training within General AI Courses*

General AI literacy training in the government should include ethical and responsible AI training. As an immediate priority, DoD, DHS, IC and FBI, as the core national security agencies and departments that utilize AI, should integrate ethical and responsible AI considerations into their general training programs.

*Action/Implementation*

This recommendation is aligned with the training recommendation in Tab 3. As we describe there, Congress should direct the above departments and agencies to create a mandatory training program for their employees that addresses, among other things, baseline instruction in the nature, development, limitations, and application of AI and data science and the basics of data management. Instruction related to the responsible and ethical development and fielding of AI should also be included.

With respect to certified self-development courses that employees may elect to take, the agencies listed above—as well as the State Department and the Commerce Department's Bureau of

Industry and Security—should develop a list of approved online courses related to AI. Lists should include at least one course addressing the ethical and responsible use of AI.

## Recommendation 2: Share Courses on Ethical and Responsible AI with Law Enforcement

State, local, tribal, and territorial law enforcement entities that are engaged in joint missions with DHS and FBI also need situational awareness on ethical and responsible AI considerations. To this end, DHS and the FBI should offer to share courses covering ethical and responsible AI considerations through existing partnerships, such as the National Network of Fusion Centers.[135]

### *Proposed Legislative Branch Action*

Congress should require that the Secretary of Homeland Security and the Director of the Federal Bureau of Investigation share their ethical and responsible AI training programs with state, local, tribal, and territorial law enforcement officials through the National Network of Fusion Centers. DHS and FBI should keep a record of those jurisdictions that avail themselves of the offered training, and report this information to Congress annually for five years.

## Recommendation 3: Establish an expert body to brief the Federal government on emerging issues in AI ethics and responsibilities.

AI is a rapidly evolving field and policies surrounding it require continuous review and updating. The Federal government is unable to effectively keep pace with these changes. To assist in diffusing the latest developments related to ethical and responsible AI, outside help is necessary. Congress should require that NIST and NSF establish a Board that would, at a minimum, provide an annual brief to certain members of the national security workforce on emerging considerations for ethical and responsible AI. Briefers should have practical expertise on ethical and responsible AI considerations, including both emerging concerns and best practices. Since a core aspect of responsible AI is technical best practices, this expert body should be convened by NIST and NSF. To bring in outside expertise on emerging ethical and responsible AI considerations, NIST and NSF should convene, at a minimum, representation from civil society, academia (including non-technical representatives in the psychological, sociological, and ethical fields), and Federally Funded Research and Development Centers (FFRDCs).

The audience for this briefing should include nominated members from DoD, the IC, DHS, and FBI, including procurement officers, legal advisors, technologists, Designated Agency Ethics Officials, and Inspectors General. The end goal is for these "trainees" to take knowledge back to their home agencies, serve as informed voices that could identify ethical concerns with AI systems, and assist in the development and fielding of ethical and responsible AI.

### *Proposed Legislative Branch Action*

Congress should require that the Director of the National Institute of Science and Technology (NIST), in collaboration with the Director of the National Science Foundation (NSF), establish a

[135] See, e.g., Department of Homeland Security, *Fusion Centers*, https://www.dhs.gov/fusion-centers.

voted upon Board of interdisciplinary experts qualified to speak on emerging considerations for ethical and responsible AI. Board members shall be voted upon annually for one-year term positions. These members must come from diverse backgrounds (at a minimum, representation from civil society; academia, including non-technical representatives in psychological, sociological, and ethical fields; and FFRDCs). Even after the completion of the Board voting process, NIST and NSF shall retain the option to call upon additional experts to be included as briefers to address ethical issues that might arise throughout the year.

This body should provide, at a minimum, an annual brief on emerging concerns and best practices for ethical and responsible AI to nominated members from DoD, the IC, DHS, and FBI, including procurement officers, legal advisors, technologists, Designated Agency Ethics Officials and Inspectors General.

NIST should memorialize the briefing and ensuing teachings for distribution to the USG writ large through channels it deems most appropriate (e.g., in white papers or on its website).

## ISSUE #2: DOCUMENTATION ON DATA, MODELS, AND SYSTEMS

In the Commission's Interim Report, we noted that auditability is a core requirement for trustworthy AI systems. Auditability, in turn, is made possible through traceability, which is also listed as an essential AI Ethics Principle by DoD. Traceability and auditability together allow for accountability.

These AI ethics principles—traceability, auditability, accountability—are all supported by data, model, and system documentation. Incorporating documentation into engineering practices makes it more feasible to provide assurances of both ethical alignment and operational integrity of our AI systems. Without such documentation, AI systems would remain opaque and responsible AI would not be achieved. More specifically, these documentation practices allow for the visibility into data and model quality and characteristics, even as the chain of custody for data and models changes. Parties interfacing with data and models must know key criteria about them to know if they are responsible and appropriate to use in a given context.[136] As more robust and mature methods to ensure the traceability and auditability of AI models are developed, documentation will make it more feasible to apply those methods to existing models.

Design documentation should include data, model, and system documentation.[137] Data documentation at a minimum must reveal what the data is; why, how, and from whom it was collected; and what the data can be appropriately used for.[138] Such information helps stakeholders

[136] For instance, data might have been collected for an explicit purpose and not be appropriate to use in another context. Likewise a model may be tested to perform reliably under a given set of noted conditions, but would not be appropriate to use in a drastically different context.

[137] For one example of a commendable effort at producing an auditing and documentation framework, see Inioluwa Deborah Raji, et al., *Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing*, Proceedings of the January 2020 Conference on Fairness, Accountability, and Transparency (Jan. 2020), https://dl.acm.org/doi/abs/10.1145/3351095.3372873.

[138] Departments and agencies have long-standing, significant data-handling requirements, some of which may already address the concerns listed above and could be integrated into a documentation strategy. See Office of the Director of National Intelligence, *Intelligence Community Information Environment Data Strategy* (2017), https://www.dni.gov/files/documents/CIO/Data-Strategy_2017-2021_Final.pdf; or Office of the Director of National Intelligence, *Access Rights and Handling*, https://www.dni.gov/index.php/who-we-

identify not only if a given dataset is operationally relevant, but also if it is appropriate to use per ethical and legal privacy commitments. Model documentation may describe what the model is (e.g., its parameters and weights), and characteristics/comments about its training, testing process, and results. System documentation captures how datasets and models within an AI system are connected, potential complications that may surface from the connections, and how the complications are accounted for. This information on models and systems is essential for operational integrity and will further ethical and legal commitments to fairness. For instance, the documentation may identify a model's performance metrics and constraints, including measures of fairness. We note that there is not a single definition of fairness of AI systems. Assumptions about the specific definition of fairness being pursued need to be decided, asserted, and disclosed.

Documentation on data, models, and systems provides transparency to those who will be developing, approving, accessing, and maintaining these systems, as well as to those conducting oversight and testing of such systems.

## *Recommendation 4: Develop Strategies for Documentation*

DoD, DHS, the IC and FBI should coordinate on a single documentation strategy for all future datasets, AI models, and systems. Examples of such a strategy can be found in the multiparty stakeholder ABOUT ML[139] effort. Having a single documentation strategy is critical to allow for interoperability among these agencies.

We recommend that NIST lead this coordination of DoD, DHS, the IC, and FBI to develop a documentation strategy, including documentation requirements, for any future AI-related datasets, models, and systems that are acquired, developed, and/or used. Documentation requirements must include documentation of the origins of datasets and their intended use; model performance and testing; connections between and dependencies within systems, and associated potential complications; and ongoing maintenance requirements. Each department/agency should incorporate documentation strategy requirements into their future procurement requirements. As appropriate, consistent with current classification protocols for documentation, some IC entities might need to have appropriate classifications for documentation requirements. Documentation requirements should be met so as to not infringe upon vendor IP rights.

## *Recommendation 5: Conduct Agency Self-Assessments on Resources for Documentation*

DoD, the IC, DHS, and FBI should conduct individual self-assessments to determine if they have adequate resources to support the documentation practices described above. If an agency determines that adequate resources do not currently exist, the agency should identify the additional resources needed and request an appropriation from Congress.

*Proposed Legislative Action for Recommendations 4 and 5*

are/organizations/enterprise-capacity/ic-cio/ic-cio-related-menus/ic-cio-related-links/ic-technical-specifications/access-rights-and-handling.

[139] See Annotation and Benchmarking on Understanding and Transparency of Machine learning Lifecycles (ABOUT ML), an evolving body of work from the Partnership on AI about documentation best practices, at https://www.partnershiponai.org/about-ml/.

Congress should require that the following actions occur within the next year to move the national security agencies forward to incorporate best practices for AI documentation.

- NIST should lead the development and publication of the kind of AI documentation strategy described above. This should be in consultation with parties including agency designees from the DoD, the IC, DHS and FBI as well as the broader AI community. In doing so, NIST and convened parties should consider documentation requirements such as: documentation of the origins of datasets and their intended use; model performance and testing; connections between and dependencies within systems, and associated system complications; and ongoing maintenance requirements.
- After NIST publishes the strategy, the agencies should implement it, including by incorporating these documentation standards and requirements into future procurement requirements. If the agency does not have the authorities or resources necessary to effectively incorporate the strategy, the head of the department or agency should ask Congress for assistance.
- To the extent that an organization fails to incorporate the strategy in a timely fashion, Congress should further mandate the incorporation of the documentation strategy and requirements.

## ISSUE #3: RESPONSIBLE PROCUREMENT

To responsibly procure AI systems, an understanding of the technology, including capabilities and limitations, as well as ethical considerations and legal implications is critical. Without understanding the nuances of the technology (e.g., the potential for unwanted bias to enter beyond training data selection, or the potential for re-identification of personally identifiable information (PII) after data has been anonymized), technology procurers will not know how to properly vet and discern between vendor offerings. Moreover, an understanding of the technology alone is inadequate. For example, due diligence requires an understanding of the context in which a system will be used and expertise on the legal requirements and ethical implications for that use.

The government can responsibly procure AI systems, and adequately vet them along ethical and responsible AI considerations, only if the procurement process integrates a multidisciplinary approach. An example of this best practice arises in the development context through DARPA's Urban Reconnaissance through Supervised Autonomy program, where technologists, legal experts, and ethicists are collaborating with the Institute for Defense Analyses to better inform AI design and build requirements (including adjustments to optimize compliance with international humanitarian law).[140]

DoD, the IC, DHS, and FBI are each moving towards incorporating multidisciplinary perspectives into their procurement processes. Each organization, however, is doing so at different speeds and with varying levels of depth. Given the urgency to include a wide array of expert opinions in the process of procuring AI systems, more information is needed to assess how the government can help departments access, convene, and engage with such experts. For instance, some departments and agencies may have multidisciplinary expertise in-house. DoD has ethicists within the JAIC and experts in International Humanitarian Law. In the DHS context,

[140] See DARPA, *Urban Reconnaissance through Supervised Autonomy*, https://www.darpa.mil/program/urban-reconnaissance-through-supervised-autonomy; and Defense Innovation Board, *AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense - Supporting Documen*t at 19 (Oct. 2019), https://media.defense.gov/2019/Oct/31/2002204459/-1/-1/0/DIB_AI_PRINCIPLES_SUPPORTING_DOCUMENT.PDF.

this would include Privacy and Civil Liberties experts. Other departments may not have such internal expertise, however. Even when a department does have internal experts, they might not have the processes in place to encourage or require procurement officers to access such expertise. In addition, departments without internal expertise might lack processes for procurement officers to access and engage with outside experts. In short, DoD, the IC, DHS, and FBI should provide information to identify what resources and processes could help to integrate multidisciplinary expertise into their procurement processes. It is unclear whether such information has been generated, and it is essential to making our recommendations.

## *Recommendation 6: Conduct Agency Self-Assessments of Adequate Multi-Disciplinary Support for AI Procurement*

DoD, the IC, DHS and FBI should conduct self-assessments as to whether they have access to adequate multi-disciplinary expertise (e.g., ethical, legal, and technical), and whether current procurement processes sufficiently encourage and/or require such expertise to be utilized. Organizations should also assess whether they have the ability and resources to bring in experts for consultation when a need is identified for expertise beyond what is available in-house. If adequate resources do not exist, the organization should report to Congress on any additional resources or congressional support needed.

The respective self-assessment must contain metrics, both qualitative and quantitative, that capture the current state of involvement of multidisciplinary experts in the procurement process. For instance, quantitative metrics might include the number of individuals or disciplines that are consulted and the funding available to bring outside experts to consult on procurement issues. Qualitative metrics could include a description of the processes that allow multidisciplinary experts to be incorporated into the procurement process and a description of the quality and consistency of such consultations. If inadequate processes exist, agencies should note how they could be improved.

### *Proposed Legislative Branch Action*

Congress should require that the Secretary of Defense, the Director of National Intelligence, the Secretary of Homeland Security and the Director of the Federal Bureau of Investigation conduct self-assessments for their departments and agencies as to whether adequate resources and processes exist for consulting multi-disciplinary experts, be they in-house or external, in the procurement process. If resources or processes are inadequate, the above secretaries and directors should inform Congress of the shortfalls and additional support required.

# *Quarter 1 Funding Table*

## Appendix A

| Category | Recommendation & Description | Cabinet Departments and Major Agencies | Amount |
|---|---|---|---|
| Tab 1: Research and Development | 1....... Topline Increase for Additional AI R&D | National Science Foundation | $450 million |
| | 1....... Topline Increase for Additional AI R&D | Department of Energy | $200 million for DOE non-defense discretionary |
| | 1....... Reprioritization for AI R&D | Department of Energy National Nuclear Security Administration | $100 million |
| | 1....... Topline Increase for Additional AI R&D | National Institutes of Health | $125 million |
| | 1....... Topline Increase for Additional AI R&D | National Aeronautics and Space Administration | $75 million |
| | 1....... Topline Increase for Additional AI R&D | National Institute of Standards and Technology | $50 million |
| | 1....... Topline Increase for AI Awards and Fellowships: DOE's Early Career Research Program and Computational Graduate Program | Department of Energy | $3 million for Early Career Research Program and $2 million for Computational Science Graduate Fellowship ($5 million total) |
| | 1....... Topline Increase for AI Awards and Fellowships: NASA Space Technology Research Fellowship | National Aeronautics and Space Administration | $20 million |
| | 1....... Topline Increase for AI Awards and Fellowships: National Science Foundation CAREER fellowship; Graduate Research Fellowship Program; Cybercorps: Scholarship for Service; Historically Black Colleges and Universities Undergraduate Program; National Science Foundation Research Traineeship | National Science Foundation | $36 million for CAREER fellowship; $14 million for Graduate Research Fellowship Program; $6 million for Cybercorps: Scholarship for Service; $4 million for Historically Black Colleges and Universities Undergraduate Program; and $3 million for National Science Foundation Research Traineeship ($79 million total) |
| | 1....... Reprioritization for AI Awards and Fellowships: DARPA Young Faculty Award; Vannevar Bush Faculty Fellowship; SMART Scholarship Program; National Defense Science and Engineering Graduate fellowships; Historically Black Colleges/Universities and Minority-Serving Institutions Research and Education Program | Department of Defense | $21 million in defense-wide RDT&E funding for additional AI-related fellowship and scholarship awards through the following programs: $2 million for DARPA Young Faculty Award; $3 million for Vannevar Bush Faculty Fellowship; $7 million for SMART Scholarship program; $6 million for National Defense Science and Engineering Graduate Fellowship; and $3 million for Historically Black Colleges/Universities and Minority-Serving Institutions Research and Education Program ($21 million total) |
| | 3....... Topline Increase for NSF Joint Task Force with OSTP on Five Year National AI Research Resource Pilot Program | National Science Foundation | $25 million |

| Category | Recommendation & Description | Cabinet Departments and Major Agencies | Amount |
|---|---|---|---|
| Tab 3: Workforce | 2....... Reprioritization for short course for HR professionals, hiring managers, and recruiters | Department of Defense | $2.5 million |
| | 3....... Reprioritization for referral bonuses for software development, data science, and AI experts | Department of Defense | $100,000 per Service and OSD ($500,000 total) |
| | 8....... Reprioritization for AI annual mandatory training | Department of Defense | $20 million |
| | 8....... Topline Increase for AI annual mandatory training | Department of Homeland Security | $20 million |
| | 9....... Reprioritization for self-development AI online courses and compensation | Department of Defense | $20 million |
| | 9....... Reprioritization for self-development AI online courses and compensation | Office of the Director of National Intelligence | $20 million |
| | 9....... Topline Increase for self-development AI online courses and compensation | Department of Homeland Security | $20 million |
| | 9....... Topline Increase for self-development AI online courses and compensation | Department of State | $5 million |
| | 9....... Topline Increase for self-development AI online courses and compensation | Department of Commerce | $5 million |
| | 9....... Topline Increase for self-development AI online courses and compensation | Department of Justice (Federal Bureau of Investigation) | $5 million |
| | 10.... Reprioritization for coding proficiency test | Department of Defense | $3 million |
| | 10.... Reprioritization for coding language incentive pay | Department of Defense | $1.25 million for each Military Department and the U.S. Marine Corps; $500,000 for OSD ($5.5 million total). |
| | 12.... Reprioritization for part-time AI experts from universities | Department of Defense | Such sums as necessary |
| | 12.... Topline Increase for part-time AI experts from universities | Department of Energy | Such sums as necessary |
| | 12.... Topline Increase for part-time AI experts from universities | Office of the Director of National Intelligence | Such sums as necessary |
| Tab 4: Hardware and 5G | 1-1... Reprioritization for AI multi-chip package demonstration program | Department of Defense | $50 million |
| | 1-2... Reprioritization for site survey for split manufacturing | Office of the Director of National Intelligence | Such sums as necessary |
| | 1-3... Fully fund DoD's Trusted and Assured Microelectronics Program FY 21 request | Department of Defense | $597 million |
| | 2-2... Reprioritization for DARPA's Electronics Resurgence Initiative | Department of Defense | $500 million total |
| | 2-3... Topline Increase NSF Funding for Microelectronics and Semiconductors* | National Science Foundation | $50 million |
| | 2-4... Reprioritization for Intelligence Advanced Research Projects Agency AI-enabled hardware challenge | Office of the Director of National Intelligence | $20 million |

**$50 million for NSF AI-enabling microelectronics is included in Tab 1 $450 million total topline increase for NSF additional AI R&D*

Note: Classified Funding Recommendations Transmitted Separately

# *Legislative Language*

## Appendix B

*The below legislative text represents the Commission staff's best effort to capture the Commissions' first quarter recommendations, and is primarily for the purposes of the National Defense Authorization Act. The Commission defers to the House and Senate members, staff, and legislative counsels as to appropriate drafting and policy.*

## TAB 1 LEGISLATIVE LANGUAGE

## *Recommendation 3: Launch a Task Force Study and Pilot Program to Establish a National AI Research Resource.*

**SEC. ___. – TASK FORCE AND PILOT PROGRAM TO ESTABLISH A NATIONAL ARTIFICIAL INTELLIGENCE RESEARCH RESOURCE. –**

(a) TASK FORCE. –

(1) ESTABLISHMENT. -- Not later than 30 days after the date of the enactment of this Act, the Director of the National Science Foundation and the Director of the Office of Science and Technology Policy shall jointly establish a task force to develop, implement, and sustain a National Artificial Intelligence Research Resource pilot.

(2) MEMBERSHIP. – The task force shall be co-chaired by the Director of the National Science Foundation and the Director of the Office of Science and Technology Policy, who shall select additional members from the following categories:

(A) representatives of federal agencies with expertise in artificial intelligence or the potential to contribute data sets to the National Artificial Intelligence Research Resource; and

(B) artificial intelligence experts from the academic and commercial artificial intelligence communities.

(3) PURPOSE. – The purpose of the task force shall be to produce, within 180 days –

(A) a roadmap laying out ownership, governance, capabilities, and sustainment requirements for a National Artificial Intelligence Research Resource that provides researchers and students with access to compute resources, co-located with artificial intelligence-ready government and non-government data sets, educational tools, and user support; and

(B) the parameters for a pilot program to accelerate and strengthen open artificial intelligence research across the U.S. and remove high-cost barriers to entry by implementing the National Artificial Intelligence Research Resource pilot over a period of five years.

(b) TRANSITION. –

(1) Upon the completion of the work of the Task Force established pursuant to subsection (a), funding and responsibility for implementation of the National Artificial Intelligence Research Resource through a multi-year pilot program shall transition to the responsible agency or agencies determined through the study.

(2) Initial implementation of the National Artificial Intelligence Research Resource shall be conducted through a five-year pilot program, which shall be designed to provide a proving ground for developing data interface and quality standards, curation best practices, anonymization techniques, and standardized procedures and criteria for determining which government and non-government data can be made publicly available under what conditions.

(3) Funding for the pilot program shall be sufficient to provide staffing necessary to implement the roadmap, maintain and improve the architecture solution, curate data sets, build interfaces and tools, and provide support to students and researchers as they use the National Artificial Intelligence Research Resource. Appropriated funds may be augmented by funding provided by private contributions and through public-private partnerships.

(c) DEFINITIONS – As used in this section:

(1) The National Artificial Intelligence Research Resource means a cloud-based system that provides researchers and students across scientific fields and disciplines with access to compute resources, co-located with publicly-available, artificial intelligence-ready government and non-government data sets and a research environment with appropriate educational tools and user support. The National Artificial Intelligence Research Resource may be realized as a single cloud resource or a federation of resources, as determined in the roadmap developed by the Task Force.

(2) Ownership means responsibility and accountability for the implementation, deployment, and ongoing development of the National Artificial Intelligence Research Resource, and for providing staff support to that effort. Ownership may be assigned to a single agency or organization, or divided among agencies or organizations, as determined in the roadmap developed by the Task Force.

(3) Governance means the processes and organizations responsible for establishing strategic direction, making programmatic decisions, managing the allocation of resources, and providing oversight for the National Artificial Intelligence Research Resource. Governance includes but is not limited to defining the grant-making selection and allocation processes, selecting government and non-government artificial intelligence-ready datasets to add to the National Artificial Intelligence Research Resource over time, and determining permissions and management of access to the data and resources hosted on the platform.

(4) Capabilities means the functions, qualities and capacities of the National Artificial Intelligence Research Resource. Relevant capabilities may include –

(A) scalability;

(B) secured access control;

(C) resident data engineering and curation expertise;

(D) provision of data sets that are findable, accessible, interoperable, and reusable;

(E) computation on hosted data that does not leave the platform;

(F) educational tools and services; and

(G) a user interface portal.

(5) Sustainment means the support and maintenance of the National Artificial Intelligence Research Resource. Sustainment may be provided through a combination of federal funding and public-private partnerships that can support provision of scalable cloud resources and a staff of cloud architects, data engineers, and educational and technical support, all at a minimal cost to the researcher or student.

# TAB 2 LEGISLATIVE LANGUAGE

## *Recommendation 1: DoD and the Office of the Director of National Intelligence (ODNI) should establish a Steering Committee on Emerging Technology tri-chaired by the Deputy Secretary of Defense, the Vice Chairman of the Joint Chiefs of Staff, and the Principal Deputy Director of ODNI.*

**SEC. ___. STEERING COMMITTEE ON EMERGING TECHNOLOGY. –**

(a) IN GENERAL. –

(1) There is established an inter-agency steering committee on emerging technology and national security threats.

(2) The steering committee is composed of the following:

(A) the Deputy Secretary of Defense, the Vice Chairman of the Joint Chiefs of Staff, and the Principal Deputy Director of National Intelligence, who shall serve as tri-chairs of the committee; and

(B) any other appropriate officials of the Department of Defense and the intelligence community, as jointly agreed upon by the tri-chairs.

(3) The Department of Defense and the Office of the Director of National Intelligence shall supply appropriate staff and resources to provide administrative support and services to the steering committee.

(b) RESPONSIBILITIES. – In addition to such other duties as may be jointly assigned by the Secretary of Defense and the Director of National Intelligence, the steering committee shall be responsible for --

(1) developing a strategic vision for organizational change, concept and capability development, and technology investments in emerging technologies such as artificial intelligence and machine learning, quantum computing, autonomy, robotics, bio-technology, nanotechnology, and other appropriate technologies needed to maintain the technological edge of the United States military and intelligence community;

(2) providing credible assessments of emerging threats and identifying adversary investments and advances in emerging technologies such as artificial intelligence and machine learning, quantum computing, autonomy, robotics, bio-technology, nanotechnology, and other appropriate technologies;

(3) making recommendations to the Secretary of Defense and the Director of National Intelligence on steps that should be taken to carry out the strategy developed pursuant to paragraph (1) and address the threats identified pursuant to paragraph (2).

## *Recommendation 2: The Director of the Joint Artificial Intelligence Center (JAIC) should report directly to the Secretary of Defense, who may delegate this authority to the Deputy Secretary of Defense.*

**SEC. ___. – ORGANIZATIONAL PLACEMENT OF DIRECTOR OF THE JOINT ARTIFICIAL INTELLIGENCE CENTER. –**

(a) DIRECT REPORTING TO SECRETARY OF DEFENSE. --

(1) The Secretary of Defense shall exercise authority and direction over the Joint Artificial Intelligence Center. The Secretary's authority under this section may not be delegated below the level of the Deputy Secretary of Defense.

(2) The Director of the Joint Artificial Intelligence Center shall report directly to the Secretary or the Deputy Secretary of Defense on matters relating to artificial intelligence policy, priorities, practices, and resourcing.

## *Recommendation 3: Maintain the Director of the JAIC as a three-star general or flag officer with proven operational experience.*

**SEC. ___. – GRADE OF DIRECTOR OF THE JOINT ARTIFICIAL INTELLIGENCE CENTER. –** An officer appointed to serve as Director of the Joint Artificial Intelligence Center shall, while so serving, have the grade of lieutenant general or vice admiral, as appropriate.

# TAB 3 LEGISLATIVE LANGUAGE

## *Recommendation 1: Expand the Cyber Excepted Service*

**SEC. __. – EXCEPTED SERVICE AUTHORITY FOR CYBER AND ARTIFICIAL INTELLIGENCE FUNCTIONS. –**

(a) AMENDMENT TO AUTHORITY FOR CYBER EXCEPTED SERVICE. – Section 1599f of title 10, United States Code, is amended –

(1) By revising the title to state: "RECRUITMENT AND RETENTION FOR UNITED STATES CYBER COMMAND AND DEPARTMENT OF DEFENSE JOINT ARTIFICIAL INTELLIGENCE CENTER";

(2) By striking subsection (a)(1) and inserting the following: "establish, as positions in the excepted service, such qualified positions in the Department of Defense as the Secretary determines necessary pursuant to paragraph (2).";

(3) By redesignating paragraph (2) as paragraph (3);

(4) By inserting before paragraph (3) the following:

"(2) The positions referred to in paragraph (1) are:

"(A) positions that the Secretary determines necessary to carry out the responsibilities of the United States Cyber Command, including –

"(i) positions held by staff of the headquarters of the United States Cyber Command;

"(ii) positions held by elements of the United States Cyber Command enterprise relating to cyberspace operations, including elements assigned to the Joint Task Force-Department of Defense Information Networks; and

"(iii) positions held by elements of the military departments supporting the United States Cyber Command; and

"(B) positions that the Secretary determines necessary to carry out the responsibilities related to artificial intelligence, as defined in paragraph (7) of subsection (k), including –

"(i) positions held by staff of the Joint Artificial Intelligence Center;

"(ii) positions held by elements of the Joint Artificial Intelligence Center related to artificial intelligence;

"(iii) positions held by all other elements of the Office of the Secretary of Defense and Defense Activities and Field Agencies related to artificial intelligence; and

"(iv) positions held by elements of the military departments related to artificial intelligence.";

(5) In subsection (b)(1)(A), by striking "the cyber mission of the Department" and inserting "the cyber and artificial intelligence missions of the Department";

(6) By amending subsection (d) to read as follows:

"(d) IMPLEMENTATION PLAN REQUIRED. – The authority granted by subsection (a) with regard to positions that the Secretary determines necessary to carry out responsibilities related to artificial intelligence shall become effective 30 days after the date on which the Secretary of Defense provides to the congressional defense committees a plan for implementation of such authority. The plan shall include the following:

"(1) An assessment of the current scope of the positions covered by the authority.

"(2) A plan for extending to positions described in paragraph (2)(B) the personnel authorities and systems that are applicable to positions described in paragraph (2)(A).

"(3) An assessment of the anticipated workforce needs of the Joint Artificial Intelligence Center across the future-years defense plan.

"(4) Other matters as appropriate."

(7) By amending subsection (h) to add at the end the following:

"(3) Each report submitted under this subsection shall differentiate between employees serving in positions described in paragraph (2)(A) of subsection (a) and employees serving in positions described in paragraph (2)(B) of such subsection."; and

(8) In subsection (k), by adding at the end the following:

"(7) The term 'artificial intelligence' includes each of the following:

"(A) Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.

"(B) An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.

"(C) An artificial system designed to think or act like a human, including cognitive architectures and neural networks.

"(D) A set of techniques, including machine learning that is designed to approximate a cognitive task.

"(E) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision-making, and acting."

## *Recommendation 2: Increase Human Resource Team AI Literacy*

**SEC. __. – INCREASING HUMAN RESOURCE TEAM LITERACY IN ARTIFICIAL INTELLIGENCE. –**

(a) DEPARTMENT OF DEFENSE. –

(1) Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall develop a training and certification program on software development, data science, and artificial intelligence that is tailored to the needs of the covered human resources workforce.

(2) The course required by paragraph (1) shall –

(A) Provide a generalist's introduction to software development and business processes, data management practices related to machine learning, machine learning, deep learning, and artificial intelligence, and artificial intelligence workforce roles; and

(B) Address hiring options and processes available for software developers, data scientists, and artificial intelligence professionals, including but not limited to direct hiring authorities, excepted service authorities, the Intergovernmental Personnel Act, and authorities for hiring special government employees and highly qualified experts.

(3) It shall be the objective of the Department of Defense to provide the training course developed pursuant to paragraph (1) to the covered human resources workforce in such a manner that:

(A) In the first year, 20 percent of the workforce is certified as having successfully completed the course; and

(B) In each year thereafter an additional 10 percent of the workforce is certified, until the Department achieves and maintains a status in which 80 percent of the covered human resources workforce is so certified.

(b) OTHER NATIONAL SECURITY AGENCIES. – The Secretary of Defense shall work with the Attorney General, the Secretary of Homeland Security, the Director of National Intelligence, or the head of any element of the Intelligence Community to offer the training and certification program developed pursuant to subsection (a) to employees of other national security agencies and to encourage the heads of such agencies to achieve a level of certification comparable to the objectives established for the Department of Defense.

(c) DEFINITION. – In this section, the term "covered human resources workforce" means human resources professionals, hiring managers, and recruiters who are or will be responsible for hiring software developers, data scientists, or artificial intelligence professionals.

(d) AUTHORIZED FUNDING. – The Secretary of Defense is authorized to expend up to $2,500,000 for the purpose of developing the training and certification program required by subsection (a) and providing the course to Department of Defense employees.

## *Recommendation 3: Rebalance the Hiring Triangle*

**Sec. ___. – GUIDANCE AND DIRECTION ON USE OF DIRECT HIRING PROCESSES FOR ARTIFICIAL INTELLIGENCE PROFESSIONALS AND OTHER DATA SCIENCE AND SOFTWARE DEVELOPMENT PERSONNEL.**

(a) IN GENERAL. – Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall issue guidance to the secretaries of the military departments and the heads of the defense components on improved use of the direct hiring processes for artificial intelligence professionals and other data science and software development personnel. The objective of the guidance shall be to ensure that organizational leaders assume greater responsibility for the results of civilian hiring of artificial intelligence professionals and other data science and software development personnel.

(b) CONTENTS OF GUIDANCE. – At a minimum, the guidance required by subsection (a) shall --

(1) Instruct human resources professionals and hiring authorities to utilize direct hiring authorities (including excepted service authorities) for the hiring of artificial intelligence professionals and other data science and software development personnel, to the maximum extent practicable;

(2) Instruct hiring authorities, when using direct hiring authorities, to prioritize utilization of panels of subject matter experts over human resources professionals to assess applicant qualifications and determine which applicants are best qualified for a position;

(3) Authorize and encourage the use of ePortfolio reviews to provide insight into the previous work of applicants as a tangible demonstration of capabilities and contribute to the assessment of applicant qualifications by subject matter experts;

(4) Authorize the secretaries of the military departments and the heads of the defense components to waive qualification standards for General Schedule positions established by the Office of Personnel Management that would unnecessarily restrict the judgment of the subject matter experts as to the best qualified applicants, to the extent permitted by law; and

(5) Authorize and encourage the use of referral bonuses for recruitment and hiring of highly-qualified artificial intelligence professionals and other data science and software development personnel in accordance with volume 451 of Department of Defense Instruction 1400.25.

(c) REPORT. – Not later than one year after the date on which the guidance is issued, the Secretary shall report to the congressional defense committees on the guidance issued pursuant to subsection (a). At a minimum, the report shall address --

(1) the objectives of the guidance and the manner in which the guidance seeks to achieve those objectives;

(2) the impact of the guidance on the hiring process for artificial intelligence professionals and other data science and software development personnel, including the impact on –

(A) hiring time;

(B) the use of direct hiring authority;

(C) the use of subject matter experts; and

(D) the quality of new hires, as assessed by hiring managers and organizational leaders.

## *Recommendation 4: Grant Exemption from OPM General Schedule Qualification Policies for Specific Billets and Position Descriptions*

**SEC. ___. – WAIVER OF QUALIFICATION STANDARDS FOR GENERAL SCHEDULE POSITIONS IN ARTIFICIAL INTELLIGENCE. –**

(a) DEPARTMENT OF DEFENSE. – Two-star and above commands and their civilian equivalents are authorized to waive any General Schedule qualification standard established by the Office of Personnel Management in the case of any applicant for a position in artificial intelligence who is determined by a hiring manager, in consultation with subject matter experts, to be the best qualified candidate for the position.

(b) OTHER NATIONAL SECURITY AGENCIES. – The Director of the Office of Personnel Management shall establish a process by which the the Attorney General, the Secretary of Homeland Security, the Secretary of State, the Secretary of Commerce, the Director of National Intelligence, and the head of any element of the Intelligence Community may request an exception to any General Schedule qualification standard in any case in which the agency head determines that national security needs would best be met by hiring managers making an independent judgment about qualifications and pay grades for a position in artificial intelligence with the advice of subject matter experts. The process shall provide for requests to be made for individual billets, for position descriptions, or for categories of individual billets or position descriptions at the discretion of the agency head.

## *Recommendation 5: Accelerate Security Clearance Investigation and Adjudication*

**SEC. ___. – SECURITY CLEARANCE PRIORITY FOR ARTIFICIAL INTELLIGENCE AND RELATED POSITIONS. –**

(a) PRIORITIZATION OF ARTIFICIAL INTELLIGENCE POSITIONS. -- Notwithstanding any other provision of law, the Secretary of Defense shall prioritize applicants for positions in artificial intelligence, data science, and software development in the security clearance and adjudication process as defined in the John S. McCain National Defense Authorization Act of Fiscal Year 2019 (P.L. 115-232).

(b) EXPEDITED STANDARD. -- The Secretary shall direct the Director of the Defense Counterintelligence Security Agency to establish an objective of making determinations on clearances for persons selected for positions in artificial intelligence, data science, and software development as follows:

(1) For interim secret clearances, within 20 days of application; and

(2) For interim top secret clearances, within 30 days of application.

(c) QUARTERLY BRIEFING REQUIRED. -- The Secretary shall provide a quarterly briefing to the congressional defense committees on the timeliness of security clearance determinations under this section, and the extent to which the objectives established in subsection (b) have or have not been met.

## *Recommendation 6: Create Unclassified Workspaces*

**SEC. ___. – UNCLASSIFIED WORKSPACES PRIOR TO RECEIVING CLEARANCES. –**

(a) DEPARTMENT OF DEFENSE. – Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall issue guidance to the secretaries of the military departments and the heads of the defense components to ensure that all Department of Defense facilities in which employees perform artificial intelligence functions make workspaces available in which employees who have applied for but not yet received security clearances can perform unclassified work. The guidance shall provide for other appropriately screened personnel, including interns and visiting experts to make use of such space, subject to availability.

(b) OTHER NATIONAL SECURITY AGENCIES. – The Secretary shall work with the Attorney General, the Secretary of Homeland Security, the Director of National Intelligence, or the head of any element of the Intelligence Community to develop common standards for ensuring that national security facilities in which employees perform artificial intelligence functions make workspaces available in which employees who have applied for but not yet received security clearances can perform unclassified work. The guidance shall provide for other appropriately screened personnel, including interns and visiting experts to make use of such space, subject to availability.

## *Recommendation 7: Use ePortfolio Reviews*

**SEC. __. – PILOT PROGRAM FOR THE USE OF ePORTFOLIO REVIEWS. –**

(a) DEPARTMENT OF DEFENSE. -- Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall establish a pilot program in at least one major command of each of the military departments, pursuant to which hiring managers, in consultation with subject matter experts, will evaluate all applicants for artificial intelligence, data science, and software development positions, using ePortfolios that include examples of the applicants' best work as a basis for the assessments.

(b) OTHER NATIONAL SECURITY AGENCIES. -- The Secretary of Defense shall work with the Secretary of Homeland Security and the Director of National Intelligence to encourage other national security and intelligence agencies to undertake similar pilot programs.

(c) REPORT. -- Not later than two years after the commencement of the pilot program required by this subsection, the Secretary of Defense shall report to the congressional defense committees on the results of the pilot program. At a minimum, the report shall address the timeliness of the hiring process and the satisfaction of organization leaders, hiring authorities, and subject matter experts with the quality of applicants brought on board pursuant to the program.

## *Recommendation 8: Mandatory AI Training*

**SEC. ___. – MANDATORY ANNUAL ARTIFICIAL INTELLIGENCE LITERACY TRAINING FOR NATIONAL SECURITY WORKFORCE. –**

(a) DEPARTMENT OF DEFENSE. –

(1) Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall develop and implement --

(A) in-person or on-line training on artificial intelligence either as a separate course or through integration into existing training to provide the Department of Defense workforce a baseline familiarity with artificial intelligence as a tool and an understanding of the national security imperatives associated with developing and using artificial intelligence; and

(B) a system for tracking course participation.

(2) The course required by paragraph (1) shall --

(A) focus on end users and their ability to collect and manage data;

(B) address basic concepts of artificial intelligence, including machine learning, the capabilities and limitations of artificial intelligence, software decision-making, and probabilistic reasoning;

(C) survey current and potential future Department of Defense artificial intelligence capabilities and applications (at an unclassified level);

(D) provide an introduction to the considerations for ethical and responsible artificial intelligence; and

(E) take an iterative approach, using sequencing and repetition in annual blocks to build progressive levels of comprehension.

(3) Annual participation in the course developed pursuant to paragraph (1) shall be mandatory for all members of the military and all civilian employees of the Department of Defense for the five-year period beginning on the date on which the course is implemented by the Secretary. At the end of the five-year period, the Secretary shall assess the success of the training program and the feasibility and desirability of continuing the requirement for mandatory training.

(b) OTHER NATIONAL SECURITY AGENCIES. -- The Secretary of Defense shall work with the Secretary of Homeland Security, to make the training program developed pursuant to subsection (a) available to their employees and to encourage the heads of such agencies to achieve a level of participation comparable to the level of participation required for the Department of Defense.

(c) AUTHORIZED FUNDING. – The Secretary of Defense is authorized to expend up to $20,000,000 for the purpose of developing the training program and the participation tracking system required by subsection (a) and providing the course to Department of Defense employees.

## *Recommendation 9: Certified Self-Development*

**SEC. __. – CERTIFIED SELF-DEVELOPMENT OF ARTIFICIAL INTELLIGENCE KNOWLEDGE AND EXPERTISE.**

(a) DEPARTMENT OF DEFENSE. --

(1) Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall develop --

(A) a list of approved on-line courses related to artificial intelligence that may be taken on a voluntary basis and on their own time by members of the Department of Defense workforce;

(B) a system for certifying and documenting in personnel files the successful completion of on-line artificial intelligence courses pursuant to paragraph (A); and

(C) a system for rewarding members of the Department of Defense workforce who are certified as successfully completing one or more voluntary training courses pursuant to paragraph (A), which may include –

(i) for members of the military, a 24-hour pass which may be used on a stand-alone basis or in conjunction with other leave, holiday, or weekend periods; and

(ii) for civilian employees of the Department, up to 8 hours of leave.

(2) The Secretary of Defense is authorized to expend up to $20,000,000 for the purpose of developing and implementing the training program and tracking system required by paragraph (1).

(b) OTHER NATIONAL SECURITY AGENCIES. – The Secretary of Defense shall work with the Secretaries of Homeland Security, State, and Commerce, the Director of National Intelligence, and the Director of the Federal Bureau of Investigation to make the training, certification and tracking system developed pursuant to subsection (a) available to other national security agencies and to encourage the heads of such agencies to provide rewards for certified course completion that are comparable to those offered by the Department of Defense.

## *Recommendation 10: Measure and Incentivize Programming Proficiency*

**SEC. __. – MEASURING AND INCENTIVIZING PROGRAMMING PROFICIENCY. --**

(a) DEPARTMENT OF DEFENSE. –

(1) Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall --

(A) develop and implement a coding language proficiency test and an artificial intelligence competency test that can be used, in a manner similar to the Defense Language Proficiency Test for foreign language skills, to identify military members and employees with varying levels of quantified coding and artificial intelligence comprehension and skills;

(B) establish a tracking and documentation system for test results that is comparable to the system used for tracking and documenting foreign language competency, and use this system to take workforce coding and artificial intelligence comprehension and skills into account when making assignments; and

(C) implement a system of rewards, including appropriate bonuses and special pays, for military members and employees who perform successfully on coding proficiency and artificial intelligence competency tests and make their skills available to the Department.

(2) The Secretary of Defense is authorized to expend up to $8,500,000 for the purpose of implementing the tests and systems required by paragraph (1).

(b) OTHER NATIONAL SECURITY AGENCIES. -- The Secretary of Defense shall work with the Secretary of Homeland Security, the Attorney General, and the Director of National Intelligence or head of any element of the Intelligence Community to make the coding language proficiency and artificial intelligence competency tests developed pursuant to subsection (a) available to other national security agencies and to encourage the heads of such agencies to implement tracking and reward systems that are comparable to those offered by the Department of Defense.

## *Recommendation 11: Adjust the ASVAB to Identify Computational Thinking*

**SEC. ___. – MODIFYING THE ARMED SERVICES VOCATIONAL APTITUDE BATTERY TEST TO ADDRESS COMPUTATIONAL THINKING. –** Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall modify the Armed Services Vocational Aptitude Battery test to add a new subtest addressing computational thinking skills relevant to military applications, including problem decomposition, abstraction, pattern recognition, analytical ability, the identification of variables involved in data representation, and the ability to create algorithms and solution expressions.  The Secretary shall use the results of the new subtest in the same manner as the results of existing subtests to place personnel in career fields and to identify candidates for further training.

## *Recommendation 12: Create Opportunities for Students to be Exposed to Government Work by Hiring University Professors as Part-Time Government Researchers*

**SEC. ___. – PROGRAM FOR PART-TIME AND TERM EMPLOYMENT OF UNIVERSITY PROFESSORS AND STUDENTS IN NATIONAL LABORATORIES. –**

(a) DEPARTMENT OF ENERGY. –

(1) Not later than 180 days after the date of the enactment of this Act, the Secretary of Energy shall establish a program to provide part-time or term employment conducting research projects in the Department of Energy National Laboratories for --

(A) university professors with expertise in science, technology, engineering and mathematics; and

(B) students assisting such professors in the research projects.

(2) The Directors of the National Laboratories shall select professors for participation in the program established pursuant to paragraph (1) on the basis of –

(A) the academic credentials and research experience of the applicant;

(B) the potential contribution of the proposed research to the Department of Energy objectives; and

(C) the qualifications of any students assisting the professor in the research and the role and credentials of such students.

(3) The Secretary shall establish at least ten positions for professors under the program established pursuant to paragraph (1) in the first year. At least five of such positions shall be reserved for professors conducting research in the area of artificial intelligence and machine learning.

(4) In carrying out the hiring program established pursuant to paragraph (1), the Secretary of Energy and the Directors of the Department of Energy national laboratories may –

(A) use any hiring authority available to the Department of Energy or the operator of the national laboratory;

(B) utilize cooperative research and development agreements under section 3710a of title 15, United States Code, to enable sharing of research and expertise with universities and the private sector; and

(C) provide referral bonuses to program participants who identify students to assist in a research project under the program or to participate in laboratory internship programs and the Pathways Internship Program.

(5) The Secretary shall report to Congress on the progress of the program not later than one year after the date of the establishment of the program and every year thereafter for two years.

(A) The first report shall address, at a minimum, the number of university professors and students employed under the program, the National Laboratories employing such professors and students, and the types of research conducted or to be conducted by such professors or students.

(B) In addition to the matter covered in the first report, the second and third reports shall address the number of college interns and recent graduates hired pursuant to references by program participants and the results of the research conducted under the program to date.

(6) For the purpose of this subsection, the term "National Laboratory" has the meaning given such term in section 2 of the Energy Policy Act of 2005, 42 U.S.C. Section 15801.

(b) DEPARTMENT OF DEFENSE. –

(1) Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall establish a program to provide part-time or term employment conducting research projects in the Department of Defense science and technology laboratories for --

(A) university professors with expertise in science, technology, engineering and mathematics; and

(B) students assisting such professors in the research projects.

(2) The Directors of the science and technology laboratories shall select professors for participation in the program established pursuant to paragraph (1) on the basis of –

(A) the academic credentials and research experience of the applicant;

(B) the potential contribution of the proposed research to the Department of Defense objectives; and

(C) the qualifications of any students assisting the professor in the research and the role and credentials of such students.

(3) The Secretary shall establish at least ten positions for professors under the program established pursuant to paragraph (1) in the first year. At least five of such positions shall be reserved for professors conducting research in the area of artificial intelligence and machine learning.

(4) In carrying out the hiring program established pursuant to paragraph (1), the Secretary of Defense and the Directors of the science and technology laboratories may –

(A) use any hiring authority available to the Secretary of Defense or the Director of the science and technology laboratory, including but not limited to any authority available under a laboratory demonstration program, direct hiring authority under section 1599h of title 10, United States Code, and expert hiring authority under section 3109 of title 5, United States Code;

(B) utilize cooperative research and development agreements under section 3710a of title 15, United States Code, to enable sharing of research and expertise with universities and the private sector; and

(C) provide referral bonuses to program participants who identify students to assist in a research project under the program or to participate in laboratory internship programs and the Pathways Internship Program.

(5) The Secretary shall report to Congress on the progress of the program not later than one year after the date of the establishment of the program and every year thereafter for two years.

(A) The first report shall address, at a minimum, the number of university professors and students employed under the program, the science and technology laboratories employing such professors and students, and the types of research conducted or to be conducted by such professors or students.

(B) In addition to the matter covered in the first report, the second and third reports shall address the number of college interns and recent graduates hired pursuant to references by program participants and the results of the research conducted under the program to date.

(6) For the purpose of this subsection, the term "Department of Defense science and technology laboratories" means the laboratories designated by section 1105(a) of the National Defense Authorization Act for Fiscal Year 2010.

(c) DEPARTMENT OF HOMELAND SECURITY. –

(1) Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall establish a program to provide part-time or term employment conducting research projects in the Department of Homeland Security science and technology laboratories for –

(A) university professors with expertise in science, technology, engineering and mathematics; and

(B) students assisting such professors in the research projects.

(2) The Directors of the science and technology laboratories shall select professors for participation in the program established pursuant to paragraph (1) on the basis of –

(A) the academic credentials and research experience of the applicant;

(B) the potential contribution of the proposed research to the Department of Homeland Security objectives; and

(C) the qualifications of any students assisting the professor in the research and the role and credentials of such students.

(3) The Secretary shall establish at least ten positions for professors under the program established pursuant to paragraph (1) in the first year. At least five of such positions shall be reserved for professors conducting research in the area of artificial intelligence and machine learning.

(4) In carrying out the hiring program established pursuant to paragraph (1), the Secretary of Homeland Security and the Directors of the science and technology laboratories may –

(A) use any hiring authority available to the Secretary of Homeland Security or the Director of the science and technology laboratory, including but not limited to any authority available under a laboratory demonstration program and expert hiring authority under section 3109 of title 5, United States Code;

(B) utilize cooperative research and development agreements under section 3710a of title 15, United States Code, to enable sharing of research and expertise with universities and the private sector; and

(C) provide referral bonuses to program participants who identify students to assist in a research project under the program or to participate in laboratory internship programs and the Pathways Internship Program.

(5) The Secretary shall report to Congress on the progress of the program not later than one year after the date of the establishment of the program and every year thereafter for two years.

(A) The first report shall address, at a minimum, the number of university professors and students employed under the program, the science and technology laboratories employing such professors and students, and the types of research conducted or to be conducted by such professors or students.

(B) In addition to the matter covered in the first report, the second and third reports shall address the number of college interns and recent graduates hired pursuant to references by program participants and the results of the research conducted under the program to date.

(6) For the purpose of this subsection, the term "Department of Homeland Security science and technology laboratories" means the Chemical Security Analysis Center, the National Biodefense Analysis and Countermeasures Center, the National Urban Security Technology Laboratory, the Plum Island Animal Disease Center, and the Transportation Security Laboratory.

(d) DEPARTMENT OF COMMERCE. –

(1) Not later than 180 days after the date of the enactment of this Act, the Secretary of Commerce shall establish a program to provide part-time or term employment conducting research projects in the Department of Commerce laboratories for –

(A) university professors with expertise in science, technology, engineering and mathematics; and

(B) students assisting such professors in the research projects.

(2) The Directors of the laboratories shall select professors for participation in the program established pursuant to paragraph (1) on the basis of –

(A) the academic credentials and research experience of the applicant;

(B) the potential contribution of the proposed research to the Department of Commerce objectives; and

(C) the qualifications of any students assisting the professor in the research and the role and credentials of such students.

(3) The Secretary shall establish at least ten positions for professors under the program established pursuant to paragraph (1) in the first year. At least five of such positions shall be reserved for professors conducting research in the area of artificial intelligence and machine learning.

(4) In carrying out the hiring program established pursuant to paragraph (1), the Secretary of Commerce and the Directors of the laboratories may –

(A) use any hiring authority available to the Secretary of Commerce or the Director of the laboratories, including but not limited to expert hiring authority under section 3109 of title 5, United States Code;

(B) utilize cooperative research and development agreements under section 3710a of title 15, United States Code, to enable sharing of research and expertise with universities and the private sector; and

(C) provide referral bonuses to program participants who identify students to assist in a research project under the program or to participate in laboratory internship programs and the Pathways Internship Program.

(5) The Secretary shall report to Congress on the progress of the program not later than one year after the date of the establishment of the program and every year thereafter for two years.

(A) The first report shall address, at a minimum, the number of university professors and students employed under the program, the science and technology laboratories employing such professors and students, and the types of research conducted or to be conducted by such professors or students.

(B) In addition to the matter covered in the first report, the second and third reports shall address the number of college interns and recent graduates hired pursuant to references by program participants and the results of the research conducted under the program to date.

(6) For the purpose of this subsection, the term "Department of Commerce laboratories" means the laboratories of the National Institute of Standards and Technology Laboratories, the laboratories of the National Oceanic and Atmospheric Administration, and the Institute for Telecommunication Sciences.

(e) INTELLIGENCE COMMUNITY. –

(1) Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall establish a program to provide part-time or term employment conducting research projects in the Intelligence Community laboratories for –

(A) university professors with expertise in science, technology, engineering and mathematics; and

(B) students assisting such professors in the research projects.

(2) The Directors of the Intelligence Community laboratories shall select professors for participation in the program established pursuant to paragraph (1) on the basis of –

(A) the academic credentials and research experience of the applicant;

(B) the potential contribution of the proposed research to the Department of Homeland Security objectives; and

(C) the qualifications of any students assisting the professor in the research and the role and credentials of such students.

(3) The Director of National Intelligence shall establish at least ten positions for professors under the program established pursuant to paragraph (1) in the first year. At least five of such positions shall be reserved for professors conducting research in the area of artificial intelligence and machine learning.

(4) In carrying out the hiring program established pursuant to paragraph (1), the Director of National Intelligence and the Directors of the Intelligence Community laboratories may –

(A) use any hiring authority available to the Director of National Intelligence, the head of an agency in the intelligence community, or the Director of the Intelligence Community laboratory, including but not limited to any authority available under the Defense Civilian Intelligence Personnel

System and expert hiring authority under section 3109 of title 5, United States Code;

(B) utilize cooperative research and development agreements under section 3710a of title 15, United States Code, to enable sharing of research and expertise with universities and the private sector; and

(C) provide referral bonuses to program participants who identify students to assist in a research project under the program or to participate in laboratory internship programs and the Pathways Internship Program.

(5) The Director of National Intelligence shall report to Congress on the progress of the program not later than one year after the date of the establishment of the program and every year thereafter for two years.

(A) The first report shall address, at a minimum, the number of university professors and students employed under the program, the science and technology laboratories employing such professors and students, and the types of research conducted or to be conducted by such professors or students.

(B) In addition to the matter covered in the first report, the second and third reports shall address the number of college interns and recent graduates hired pursuant to references by program participants and the results of the research conducted under the program to date.

(6) For the purpose of this subsection, the term "Intelligence Community laboratories" means National Security Agency Laboratory for Advanced Cybersecurity Research, the Applied Research Laboratory for Intelligence and Security, and any other science and technology laboratory under the jurisdiction and authority of the intelligence community.

## *Recommendation 13: Increase the Use and Utility of Pathways Internships*

**SEC. ___. – STREAMLINED AND EXPANDED PATHWAYS INTERNSHIP OPPORTUNITIES. –**

(a) EXPANDED NATIONAL SECURITY AND INTELLIGENCE COMMUNITY OPPORTUNITIES. –

(1) Not later than one year after the date of the enactment of this Act, the national security and intelligence community leaders designated in paragraph (2) shall take steps to increase the usage of the Pathways Internship program in the national security and intelligence communities (with a focus on mathematics and computer science majors) by –

(A) Ensuring the elimination of any caps on participation in the Pathways Internship program in the national security and intelligence communities; and

(B) Establishing the objective of achieving—

(i) an annual increase of twenty percent in the number of Pathways Internships, until such time as the number has doubled from the number of such internships in 2019; and

(ii) an annual increase of twenty percent in the number of Pathways Interns converting to full-time positions, until such time as the number has doubled from the number of such conversions in 2019.

(2) Each of the leaders designated for the purpose of paragraph (1) shall report to Congress on the date that is one year after the date of the enactment of this Act and every year thereafter for a period of five years on their progress in achieving the objective established in paragraph (1). Such reports shall address, at a minimum:

(A) The change in the number of Pathways Internship program participants from the three previous fiscal years to the current fiscal year;

(B) The change in the number of mathematics and computer science majors participating in the Pathways Internship program from the three previous fiscal years to the current fiscal year;

(C) The change in and overall number of conversions from the Pathways Internship Program to full-time positions from the three previous fiscal years to the current fiscal year; and

(D) The change in the number of mathematics and computer science majors who convert from the Pathways Internship Program to full-time positions from the three previous fiscal years to the current fiscal year.

(3) The leaders designated for the purpose of paragraph (1) are –

(A) the Secretary of Defense, for the Department of Defense;

(B) the Secretary of Homeland Security, for the Department of Homeland Security;

(C) the Secretary of State, for the Department of State;

(D) the Secretary of Commerce, for the Department of Commerce; and

(E) the Director of National Intelligence, for the Intelligence Community.

(b) STREAMLINED PROCEDURES FOR PROGRAM PARTICIPATION. – Not later than 180 days after the date of the enactment of this Act, the Director of the Office of Personnel Management shall modify the regulations governing the Pathways Program to–

(1) provide for the evaluation of candidates for participation in the program against agency-developed standards, instead of permitting agencies to default to the use of Office of Personnel Management qualification standards;

(2) authorize participants in the Pathways Internship Program to convert to full-time, competitive service positions if they have –

(A) Completed 220 hours of work experience acquired through the internship program while enrolled as a full-time or part-time, degree- or certificate-seeking student, subject to existing exceptions; and

(B) Completed a course of academic study, within the 365-day period preceding the appointment, at a qualifying educational institution conferring a diploma, certificate, or degree.

(c) DEFINITION. – For the purposes of this section, the Pathways Internship Program is the program authorized by Executive Order 13562 and Part 362 of Chapter 5 of the Code of Federal Regulations.

## *Recommendation 14: Expand the CyberCorps: Scholarship for Service*

**SEC. ___. – AMENDMENT TO THE FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM. –**

(a) AMENDMENTS TO TITLE 15, UNITED STATES CODE. – Section 7442 of title 15, United States Code is amended –

(1) By amending the title to read: "Federal Cyber and Artificial Intelligence Scholarship-for-Service Program";

(2) in subsection (a), by striking "industrial control system" and all that follows and inserting in lieu thereof "digital engineers, artificial intelligence practitioners, data engineers, data analysts, data scientists, industrial control system security professionals, security managers, and cybersecurity course instructors to meet the needs of the cybersecurity and artificial intelligence missions for Federal, State, local, tribal, and territorial governments.";

(3) in subsection (b), by –

(A) striking "and" at the end of paragraph (3);

(B) striking the period at the end of paragraph (4) and inserting in lieu thereof "; and"; and

(C) adding a new paragraph (5), as follows:

"(5) provide an opportunity for scholarship recipients to initiate the security clearance process at least one year before their planned graduation date."; and

(4) in subsection (c), by striking "3 years" and inserting "4 years".

(b) SAVINGS PROVISION. – Nothing in this section, or an amendment made by this section, shall affect any agreement, scholarship, loan, or repayment under section 302 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7442), in effect on the day before the date of the enactment of this section.

## *Recommendation 15: Increase the Number of Fellowships and Partnerships with Industry, and Increase the Number Focused on Artificial Intelligence and Software Development*

**SEC. ___. – ENHANCEMENT OF PUBLIC-PRIVATE TALENT EXCHANGE PROGRAMS IN THE DEPARTMENT OF DEFENSE. –**

(a) APPLICATION OF EXCHANGE AUTHORITY TO ARTIFICIAL INTELLIGENCE. – Not later than 90 days after the date of the enactment of this Act, the Secretary of Defense shall take steps to ensure that the authority for the Department of Defense to operate a public-private talent exchange program pursuant to section 1599g of title 10, United States Code, is utilized to exchange personnel with private sector entities working on artificial intelligence applications. Such application of the authority of section 1599g shall be in addition to, not in lieu of, any other application of the authority by the Department of Defense.

(b) GOALS FOR PROGRAM PARTICIPATION. – In carrying out the requirement of subsection (a), the Secretary shall seek to achieve the following objectives:

(1) In the Secretary of Defense Executive Fellows program, the nomination of an additional five uniformed service members and three government civilians by each service and by the Office of the Secretary of Defense, for sponsorship by private sector entities working on artificial intelligence applications;

(2) For the public-private talent exchange program of the Under Secretary of Defense for Acquisition and Sustainment --

(A) an additional ten government employees to work with private sector entities working on artificial intelligence applications; and

(B) an additional ten employees of private sector entities working on artificial intelligence applications to work in the Department;

(3) The establishment of the following new public-private talent exchange programs in the Office of the Secretary of Defense, comparable to the program referenced in paragraph (2) --

(A) by the Undersecretary of Defense for Research and Engineering, a program with twenty participants, focused on exchanges with private sector entities working on artificial intelligence applications;

(B) by the Chief Information Officer of the Department of Defense, a program with twenty participants, focused on exchanges with private sector entities working on artificial intelligence applications; and

(4) In the Army, Navy, and Marine Corps, the establishment of new public-private exchange programs, comparable to the Air Force Education with Industry

Program, each with twenty program participants, focused on private sector entities working on artificial intelligence applications.

(c) TREATMENT OF PROGRAM PARTICIPANTS.

(1) The military services shall take steps to ensure that participation by a service member in a program described in subsection (b)(4) is treated, for purposes of promotion boards and subsequent assignments, as equivalent to attending resident professional military education.

(2) The Secretary of Defense shall establish a Public-Private Exchange Program Billet office to temporarily hold billets for civilian employees who participate in programs described in subsection (b), ensuring that participating Department of Defense offices are able to retain their staffing levels during the period of participation.

(d) BRIEFING ON EXPANSION OF EXISTING EXCHANGE PROGRAMS. – Not later than 180 days after the date of the enactment of this Act and annually thereafter, the Secretary of Defense shall brief the Armed Services Committees of the Senate and the House of Representatives on efforts taken to expand existing public-private exchange programs of the Department of Defense and to ensure that such programs seek opportunities for exchanges with private sector entities working on artificial intelligence applications, in accordance with the requirements of this section.

## *Recommendation 2: Maintain global leadership in microelectronics by clearly stating research priorities, increasing USG R&D funding, and articulating a national strategy for microelectronics and associated infrastructure (e.g., a national microelectronics laboratory and incubator).*

### *Recommendation 2-5: Require the USG to develop a national microelectronics strategy within 180 days and assess the viability of a national microelectronics laboratory and incubator.*

**SEC. ___. – STRATEGY FOR MICROELECTRONICS. –**

(a) MICROELECTRONICS AND NATIONAL SECURITY. –

(1) Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense, in coordination with the Secretary of Energy and the Director of National Intelligence, shall develop a strategy for ensuring continued access to state-of-the-art microelectronics for national security purposes and a plan for carrying out that strategy.

(2) The strategy and plan required by paragraph (1) shall include the following elements:

(A) A strategy for harnessing cutting-edge commercial microelectronics to enhance military capacities to strengthen the ability of the Joint Force to conduct full spectrum operations and maintain a technological advantage on the battlefield.

(B) An approach to ensuring the continuing production of cutting-edge microelectronics for national security needs, including state-of-the-art node sizes, heterogeneous integration, boutique chip designs, and variable volume production capabilities.

(C) An assessment of current supply chain management practices, existing risks, and opportunities for the national security industrial base for microelectronics to mitigate such risks.

(D) A plan for increasing commercialization of DoD-developed intellectual property for commercial microelectronics research and development.

(E) Recommendations for changes in authorities, regulations, and practices, including acquisition policies, financial management, public-private partnership policies, or in any other relevant areas, that would support the achievement of the goals of the strategy.

(F) Such other matters as the Secretary of Defense, the Secretary of Energy and the Director of National Intelligence determine to be relevant.

(3) The strategy and plan developed pursuant to paragraph (1) shall specifically address the feasibility, utility, efficacy, and cost of –

(A) developing a national laboratory exclusively focused on microelectronics research and development to serve as a center for government expertise in high-performing, trusted microelectronics and a hub for federal research into breakthrough microelectronics-related technologies; and

(B) incorporating into such national laboratory a commercial incubator to provide access to funding resources, fabrication facilities, design tools, and shared intellectual property to early-stage microelectronics startups which currently face difficulties scaling due to the high costs of microelectronics design and fabrication.

(4) to the extent practicable and advisable, such strategy and plan shall include measures to implement the recommendations set forth in the Strategy for Assured Access to Trusted Microelectronics submitted to the congressional defense committees under section 231 of the National Defense Authorization Act for Fiscal Year 2017 (P.L. 114-328).

(b) MICROELECTRONICS LEADERSHIP AND COMPETITIVENESS. --

(1) Not later than 30 days after the date of the enactment of this Act, the National Security Council, in coordination with the National Economic Council and the Office of Science and Technology Policy, shall establish a senior leadership panel to develop a national strategy to accelerate the development and deployment of state-of-the-art microelectronics and ensure future U.S. leadership in the field of microelectronics.

(2) The senior leadership panel established pursuant to paragraph (1) shall be chaired by the Secretary of Commerce and shall include the Secretary of State, the Secretary of Defense, the Secretary of Energy, the Secretary of Homeland Security, the Director of National Intelligence, the Director of the National Science Foundation, the U.S. Trade Representative, and such other senior officials as the National Security Council determines to be appropriate.

(3) Not later than 180 days after it is established, the senior leadership panel shall develop a national strategy for ensuring continued U.S. leadership in high-performance microelectronics and a plan for carrying out such strategy. Such strategy and plan shall address the following:

(A) Measures to strengthen engagement and outreach with industry, academia, international partners, and other departments and agencies of the Federal Government on issues relating to microelectronics;

(B) Science, technology, research, and development efforts to facilitate the advancement and adoption of microelectronics and new uses of microelectronics and components, including—

(i) accelerating leap-ahead research, development, and innovation in microelectronics; and

(ii) deploying heterogeneously integrated microelectronics for machine learning and other applications.

(C) The role of diplomacy and trade in maintaining U.S. microelectronics leadership, including the feasibility and advisability of --

(i) multilateral export controls tailored through direct coordination with key U.S. allies, the Wassenaar Arrangement, and other multilateral fora for specific semiconductor manufacturing equipment such as extreme ultraviolet photolithography equipment and argon fluoride immersion photolithography equipment;

(ii) additional U.S. trade enforcement actions to address any unfair or excessive foreign semiconductor subsidy programs or other unfair microelectronics trade practices; and

(iii) the elimination of any trade barriers or unilateral export controls that are determined to harm U.S. companies without producing a substantial benefit to U.S. competitiveness or national security.

(D) The potential role of a national laboratory and incubator, as described in subsection (a), in carrying out the strategy and plan required by paragraph (1).

(E) Such other steps needed to overcome looming challenges to U.S. microelectronics innovation, competitiveness, and supply chain integrity as may be determined to be appropriate by the panel.

(c) Briefings.—Not later than 90 days after the date of the enactment of this Act –

(1) the Secretary of Defense shall brief the congressional defense committees on the progress of the Secretary in developing the strategy and implementation plan required under subsection (a); and

(2) the Assistant to the President for National Security Affairs shall brief the congressional defense committees on the progress of the senior leadership panel in developing the strategy and implementation plan required under subsection (b).

# TAB 6 LEGISLATIVE LANGUAGE

## *Recommendation 1: Integrate Ethical and Responsible AI Training within General AI Courses*

This recommendation is incorporated into the Tab 3, *Recommendation 8: Mandatory AI Training* legislative text.

## *Recommendation 2: Share Courses on Ethical and Responsible AI Considerations with Law Enforcement*

**SEC. ___. – SHARING OF TRAINING PROGRAMS ON ETHICAL AND RESPONSIBLE AI CONSIDERATIONS WITH STATE, LOCAL, TRIBAL, AND TERRITORIAL LAW ENFORCEMENT. –**

(a) IN GENERAL. -- The Secretary of Homeland Security and the Director of the Federal Bureau of Investigation shall --

(1) identify existing agency training programs that address the ethical and responsible use of artificial intelligence technology;

(2) make such training programs available to –

(A) other federal law enforcement agencies; and

(B) state, local, tribal, and territorial law enforcement officials with whom agency personnel are engaged in joint missions; and

(3) keep a record of those agencies and jurisdictions that have availed themselves of the offered training.

(b) Not later than one year after the date of the enactment of this Act and every year thereafter for a period of five years, the Secretary of Homeland Security and the Director of the Federal Bureau of Investigation shall report to Congress statistics on the number of agencies and jurisdictions of those agencies that have availed themselves of the offered training.

## *Recommendation 3: Establish an expert body to brief the Federal government on emerging issues in AI ethics and responsibilities.*

**SEC. ___. – EXPERT GROUP ON EMERGING CONSIDERATIONS FOR ETHICAL AND RESPONSIBLE AI. –**

(a) EXPERT GROUP –

(1) Not later than 90 days after the date of the enactment of this Act, the Director of the National Institute of Standards and Technology, in collaboration with the Director of the National Science Foundation, shall establish --

(A) an expert body of interdisciplinary professionals with practical expertise on ethical and responsible artificial intelligence considerations, including emerging concerns and best practices; and

(B) a steering committee of NIST and NSF employees to vote annually on the membership of the expert body required by subparagraph (A).

(2) Members of the expert group shall be elected to one-year, renewable terms. The Director of the National Institute of Standards and Technology, in collaboration with the Director of the National Science Foundation, shall have the right to designate additional members to address ethical issues that might arise during the course of a year.

(3) Members shall be selected to ensure representation from diverse backgrounds, including at a minimum, experts from --

(A) the National Institute of Standards and Technology and the National Science Foundation;

(B) Federally Funded Research and Development Centers;

(C) The academic community (including non-technical experts in psychological, sociological, and ethical fields); and

(D) Other elements of civil society.

(b) ANNUAL BRIEFING FOR KEY EMPLOYEES. –

(1) Not later than 90 days after the date on which the expert group required by subsection (a) is convened, and every year thereafter for a period of five years, the group shall prepare and present a briefing on considerations for ethical and responsible artificial intelligence, including emerging concerns and best practices, to agency officials designated in accordance with paragraph (2) and others invited by the Director of the National Institute of Standards and Technology.

(2) The Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence shall designate agency officials to attend the annual briefings of the expert group.

(3) Individuals shall be designated to attend the annual briefings of the expert group on the basis of their participation in or responsibility for artificial intelligence or programs enabled by artificial intelligence in their agencies. Such individuals shall include but not be limited to acquisition and procurement professionals, legal advisors, technologists, and Designated Agency Ethics Officers, Inspector General personnel, and other ethics and oversight personnel.

(4) The Director of the National Institute of Standards and Technology shall ensure that a record of each briefing presented pursuant to this section is preserved and made available for training purposes to appropriate federal agency personnel.

***Suggested Conference Report Language to Accompany Recommendation 3:***

After receiving the annual briefing as described in (b), the personnel as described in (b)(2) shall be responsible for spreading awareness of best practices for responsible artificial intelligence and the mitigation of potential ethical pitfalls within their agencies.

## *Recommendation 4: Develop Strategies for Documentation, and*

## *Recommendation 5: Conduct Agency Self-Assessments on Resources for Documentation*

**SEC. ___. – ARTIFICIAL INTELLIGENCE DOCUMENTATION STRATEGY FOR THE DEPARTMENT OF DEFENSE, THE DEPARTMENT OF HOMELAND SECURITY, THE DEPARTMENT OF JUSTICE, AND THE INTELLIGENCE COMMUNITY. –**

(a) NIST WORKING GROUP. -- Not later than 30 days after the date of the enactment of this Act, the Director of National Institute of Standards and Technology shall convene a working group to develop an artificial intelligence documentation strategy for the Department of Defense, the Department of Homeland Security, the Department of Justice, and the Intelligence Community. The working group shall be chaired by the Director of the National Institute of Standards and Technology and shall include --

(1) representatives of the Secretary of Department of Defense, the Secretary of Homeland Security, the Attorney General, and the Director of National Intelligence;

(2) as determined to be appropriate by the Director of the National Institute of Standards and Technology in consultation with the agency heads designated in paragraph (1), and artificial intelligence experts from the industry, academia, and federal government.

(b) ISSUANCE OF STRATEGY. – Not later than 180 days after the date of the enactment of this Act, the working group convened pursuant to subsection (a) shall issue an artificial intelligence documentation strategy for the Department of Defense, the Department of Homeland Security, the Department of Justice, and the Intelligence Community. The documentation strategy issued pursuant to the subsection shall –

(1) support traceability, auditability and accountability for any future datasets, models, and systems that are acquired, developed, or used by the Department of Defense, the Department of Homeland Security, the Department of Justice, and the Intelligence Community to ensure visibility into data and model quality and key characteristics even as the chain of custody for the datasets, models and systems changes over time;

(2) include standards for –

(A) data documentation, including identification of the data, the origins of the data, the intent behind the creation of the dataset, descriptive characteristics of the data, and authorized uses of the data;

(B) model documentation, including a documentation of a model’s performance metrics and constraints (such as parameters and weights), measures of fairness, training and testing processes, and results;

(C) system documentation, including documentation of connections and dependencies within and between systems, complications that may arise out of such connections and dependencies, and how these complications or dependencies have been addressed; and

(D) ongoing maintenance requirements.

(c) IMPLEMENTATION OF STRATEGY. – The Secretary of Defense, the Secretary of Homeland Security, Attorney General, the Director of National Intelligence, and the heads of agencies in the Intelligence Community shall be responsible for implementing the documentation strategy issued pursuant to subsection (b) in their respective agencies and ensuring that the acquisition of future datasets, models, and systems is conducted in compliance with such strategy.

(d) AGENCY SELF-ASSESSMENTS. – Not later than 90 days after the date on which the documentation strategy is issued pursuant to subsection (b), the Secretary of Defense, the Secretary of Homeland Security, the Attorney General, and the Director of National Intelligence shall each –

(1) Conduct a self-assessment to determine the extent to which their respective department or agency has adequate resources to implement the strategy as required by subsection (c); and

(2) In the event that an agency head determines that the agency does not have sufficient resources to implement the strategy, report to Congress on the nature and extent of the deficiency.

***Suggested Conference Report Language to Accompany Recommendation 3:***

The parties named shall work toward a documentation strategy with the purpose of applying it to national security focused entities within their agencies and departments. For example, this would include elements of the Federal Bureau of Investigation that work on national security, including but not limited to intelligence. Having a single documentation strategy is critical to allow for interoperability among the national security entities with these agencies. An example of such a documentation strategy can be found in Partnership on AI's multiparty stakeholder effort, Annotation and Benchmarking on Understanding and Transparency of Machine Learning Lifecycles (ABOUT ML).

## *Recommendation 6: Conduct Agency Self-Assessments of Adequate Multi-Disciplinary Support for AI Procurement*

**Sec. ___. Agency Self-Assessment of Resources Available to Ensure Acquisition of Ethically and Responsibly Developed Artificial Intelligence. –**

(a) SELF-ASSESSMENT REQUIRED. –

(1) Not later than 180 days after the date of the enactment of this Act, the Secretary of Department of Defense, the Secretary of Homeland Security, the Attorney General, and the Director of National Intelligence, shall each conduct a self-assessment of the resources available to their respective agencies to ensure the acquisition of ethically and responsibly developed artificial intelligence.

(2) Each self-assessment conducted pursuant to paragraph (1) shall address –

(A) The adequacy of multidisciplinary resources within the agency, including ethical, legal, and technical expertise, to ensure the acquisition of ethically and responsibly developed artificial intelligence;

(B) the ability of the agency to fill any gaps in in-house expertise by bringing in outside experts for consultation;

(C) the extent to which existing acquisition processes encourage or require the use of multidisciplinary resources to ensure the acquisition of ethically and responsibly developed artificial intelligence; and

(D) quantitative and qualitative metrics for assessing the extent to which multidisciplinary experts are engaged in the agency's acquisition of artificial intelligence.

(b) MITIGATION OF GAPS. – If the head of an agency determines that it does not have adequate access to multidisciplinary experts to ensure the acquisition of ethically and responsibly developed artificial intelligence, including adequate processes to encourage or require using these experts, the agency shall report to Congress within 30 days of completion of its self-assessment on the additional resources needed and any measures that have been taken to mitigate identified gaps in resources or expertise.

NATIONAL
SECURITY
COMMISSION
ON ARTIFICIAL
INTELLIGENCE